Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema
Vigilancia masiva y privacidad en Internet

Título
“La NSA Según las Revelaciones de Snowden”

Autor: Ing. Rafael Bonifaz
Tutor: Dr. Pedro Hecht

Año 2017
Cohorte 2016

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Rafael Bonifaz

Licencia

Este trabajo esta publicado con licencia Creative Commons: Atribución 4.0 Internacional (CC BY 4.0)

Usted es libre para:

Compartir — copiar y redistribuir el material en cualquier medio o formato
Adaptar — remezclar, transformar y crear a partir del material
Para cualquier propósito, incluso comercialmente

El licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

Atribución — Usted debe darle crédito a esta obra de manera adecuada, proporcionando un enlace a la licencia, e indicando si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo del licenciante.

No hay restricciones adicionales — Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.

Aviso

Usted no tiene que cumplir con la licencia para los materiales en el dominio público o cuando su uso esté permitido por una excepción o limitación aplicable.

No se entregan garantías. La licencia podría no entregarle todos los permisos que necesita para el uso que tenga previsto. Por ejemplo, otros derechos como relativos a publicidad, privacidad, o derechos morales pueden limitar la forma en que utilice el material.

Más información: https://creativecommons.org/licenses/by/4.0/deed.es

Resumen

En 2013, Edward Snowden filtró miles de documentos de la Agencia Nacional de Seguridad de los Estados Unidos (NSA por sus siglas en inglés) a los periodistas Glenn Greenwald y Laura Poitras. Desde entonces se han publicado decenas de reportajes periodísticos a nivel mundial que revelan programas de vigilancia masiva de alcance global.

Las filtraciones muestran que esta agencia tiene la capacidad de recolectar las comunicaciones de Internet. Cables de fibra óptica, comunicaciones satelitales y telefonía celular son algunas de los medios sobre los que la agencia recolecta información. Las grandes empresas de Internet entregan los datos sus usuarios a esta agencia. Si esto no es suficiente se recurre a los ataques informáticos para buscar la información restante.

Las comunicaciones recolectadas son procesadas en sistemas sofisticados. Los mismos permiten a los analistas de la NSA encontrar información a través de buscadores similares al de Google o DuckDuckGo que operan sobre las comunicaciones privadas de quiénes usan Internet.

Si bien la NSA sostiene que los programas de vigilancia se realizan con el fin de combatir el terrorismo. Se revelaron operaciones que muestran espionaje político y a sectores estratégicos de países alrededor del mundo. En este trabajo se enfatiza el caso de América Latina.

Palabras Claves: Snowden, espionaje, vigilancia, NSA, GCHQ

Contenido

Introducción

En el año 2013 Edward Snowden filtró miles de documentos secretos de la Agencia Nacional de Seguridad de los Estados Unidos (NSA por sus siglas en inglés) a los periodistas Glenn Greenwald y Laura Poitras. Ellos publicaron parte de estos documentos, de manera conjunta, con varios medios internacionales de comunicación. Las noticias causaron preocupación, la actividad que realizan los usuarios de Internet a nivel mundial, es almacenada de forma masiva para su análisis. Esto generó debate sobre los riesgos a la privacidad en Internet.

Desde 2013 se han publicado, y se siguen publicando, reportajes de prensa que muestran las capacidades de vigilancia de esta agencia. Cuatro años después de la primera publicación, este trabajo organiza parte de la información revelada para entender como la NSA recolecta y analiza información, así como también, algunas de las operaciones de espionaje reveladas.

Cada vez que la prensa reveló un programa de vigilancia, también publicó documentos filtrados. A diferencia de revelaciones hechas por Wikileaks donde existe un repositorio central donde se puede buscar los documentos, en este caso están dispersos en los sitios web de varios medios de comunicación. Para solucionar este problema la Unión Americana de Libertades Civiles (ACLU por sus siglas en inglés), la Fundación de la Frontera Electrónica (EFF por sus siglas en inglés) y The Courage Foundation mantienen repositorios en línea con los documentos publicados a la fecha.[1]

The Courage Foundation es una organización creada para defender a denunciantes, como Snowden, que filtran información de interés público. Al momento de escribir este trabajo el repositorio cuenta con 1530 documentos. Cada uno de estos, está enlazado con el artículo de prensa donde se lo

1 Repositorio ACLU: https://www.aclu.org/nsa-documents-search
Repositorio EFF:https://www.eff.org/nsa-spying/nsadocs
Repositorio Courage Foundation: https://edwardsnowden.com/

publicó. De esta manera se puede profundizar la investigación a través del reportaje periodístico que reveló el documento.

La metodología utilizada es de investigación bibliográfica y análisis exploratorio. La fuente primaria de información son los documentos de Snowden junto a los artículos de prensa donde se publicaron. El libro "Snowden. Sin un Lugar Donde Esconderse", escrito por Greenwald, es una fuente de primera mano con visión general sobre el funcionamiento de la NSA.

Los medios de prensa que realizaron las publicaciones analizadas en este documento incluyen a: The Guardian de Inglaterra, The Washington Post de Estados Unidos, The New York Times de Estados Unidos, Propublica de Estados Unidos, The Intercept de Estados Unidos, Der Spiegel de Alemania, L'Espresso de Italia, O Globo de Brasil y Todo Noticias de Argentina.

Adicionalmente se utilizaron otras fuentes que escribieron sobre los documentos de Snowden. Entre las más importantes se encuentra el portal Electrospaces.net y el libro "El Imperio de la Vigilancia", escrito por Ignacio Ramonet. Electrospaces.net realizó varios análisis técnicos detallados sobre los documentos que ayudan a entenderlos. Por su parte el libro de Ramonet, provee una visión sobre el impacto de la vigilancia masiva en las comunicaciones en la sociedad moderna. Además, describe el contexto histórico de la NSA más allá de los documentos de Snowden.

El libro "El Centinela Secreto: La Historia no Contada de la Agencia Nacional de la Seguridad"[2] escrito por Matthew Aid, cuenta la historia de la NSA desde finales de la segunda guerra mundial hasta inicios del siglo veintiuno. Además, ayuda a entender el origen de esta agencia y como algunas de sus prácticas ya se las realizaba varias décadas atrás.

2 Traducción propia del inglés: "The Secret Sentry: The Untold History of the National Security Agency"

El primer capítulo, de este documento, sirve para entender el contexto de las revelaciones de Snowden. Primero se relata brevemente la historia de la agencia y el impacto que hubo cuando se publicaron los primeros documentos. Luego se analizan aspectos legales que permiten a la NSA llevar acabo sus operaciones. Se finaliza el capítulo con una explicación sobre el tipo de información que la agencia recolecta y porque los metadatos son igual o más importantes que el contenido de las comunicaciones.

El segundo capítulo es el más extenso y habla sobre las formas en que la NSA recolecta información. Lo hace a través de la cooperación con empresas tecnológicas de Estados Unidos. De forma coordinada con agencias de inteligencia de otros países. Interceptan las comunicaciones celulares de algunas ciudades donde operan misiones diplomáticas de Estados Unidos. Espían las comunicaciones satelitales desde estaciones terrestres distribuidas en el mundo. Cuando la información no es accesible por ninguno de estos medios se recurre a los ataques informáticos para obtenerla.

En el capítulo tres analiza como la NSA procesa la información recolectada para generar inteligencia. La principal herramienta se llama XKEYSCORE que funciona de forma similar a un buscador de Internet, como el de Google o Duckduckgo, pero para las comunicaciones privadas.

En el capítulo cuatro se muestran algunas de las operaciones realizadas por la NSA que no están relacionadas con la lucha contra el terrorismo. Espionaje a presidentes de todo el mundo, los sectores estratégicos de Venezuela y Brasil, y el ataque a los administradores de sistemas informáticos son algunas de las operaciones descritas.

En este trabajo no se publica nada que no se haya conocido antes. El principal aporte del mismo es juntar varias historias sueltas para tener una comprensión sistemática del funcionamiento de la agencia de vigilancia digital más grande del mundo. Se espera que sirva como una primera lectura para que futuras investigaciones profundicen el entendimiento del

funcionamiento de la NSA. Solo cuando se comprendan los riesgos de la vigilancia masiva se podrán tomar acciones para proteger la soberanía de los Estados y la privacidad de las personas.

1 Antecedentes

La NSA fue creada el 4 de noviembre de 1952 durante la presidencia de Harry Truman[3]. Esto sucedió con el objetivo de realizar inteligencia de señales[4]. Eran los tiempos de la guerra fría y Estados Unidos estaba interesado en conocer las comunicaciones de sus adversarios, en especial de la Unión Soviética. La NSA jugó un papel estratégico en los eventos militares en los qué Estados Unidos participó desde la Guerra Fría a la Guerra contra el terrorismo pasando por eventos como Vietnam o la Guerra del Golfo.[1]

La inteligencia de señales consiste en la interceptación y análisis de comunicación para generar inteligencia. En el caso de la NSA, las comunicaciones interceptadas deben estar fuera de los Estados Unidos. Sin embargo, en 2005 The New York Times realizó una investigación donde se denunció que la NSA espiaba dentro de Estados Unidos, sin orden judicial, simultáneamente, a unas 500 personas.[2]

Este escándalo fue pequeño comparado al ocurrido en junio de 2013 cuando los diarios The Guardian y The Washington Post empezaron a publicar documentos secretos de la NSA. El primer reporte de prensa denunció una orden judicial secreta[3] que demandó a la empresa Verizon a entregar diariamente todos los metadatos de sus clientes a la NSA.[4] La segunda publicación fue un escándalo a nivel mundial, puesto que habló del programa PRISM que afecta a los usuarios de empresas como Google, Facebook, Apple, Microsoft entre otras.[5] En la actualidad, con menor impacto y frecuencia se siguen publicando documentos de Snowden

La información filtrada fue entregada por Edward Snowden a los periodistas Laura Poitras y Glenn Greenwald, en un principio, a través de comunicaciones cifradas y luego de manera presencial en Hong Kong. En

---

3 Tiene sus raíces en la segunda guerra mundial cuando el ejercito de Estados Unidos junto a Reino Unido espiaba las comunicaciones de Alemania, Japón e Italia.

4 Es decir el espionaje realizado a las comunicaciones, normalmente digitales. En inglés se usa el término *SIGINT*.

ese entonces Snowden trabajaba para la empresa Buzz Allen Hamilton como contratista de la NSA donde tenía acceso a información clasificada.[6]

En Hong Kong, a más de Poitras y Greenwald se sumó Ewen MacAskill periodistas de The Guardian. Del tres al once de junio de 2013, mantuvieron reuniones periódicas con Snowden donde analizaron los documentos y se empezó a publicar en medios de comunicación. [7]

Desde entonces y de manera periódica Greenwald siguió publicando artículos referentes a los documentos de Snowden en The Guardian donde trabajó hasta octubre de 2013 cuando renunció para fundar el medio digital "The Intercept".[8] Adicionalmente Poitras y Greenwald en alianzas con distintos medios de prensa a nivel internacional donde siguieron publicando documentos.

La veracidad de los documentos nunca fue puesta en duda por el gobierno de Estados Unidos. El entonces director de la NSA, Keith Alexander dijo: "[Snowden] traicionó la confianza que habíamos depositado en él. Era un individuo que tenía acceso a documentos de máximo secreto y su deber era administrar las redes. Él traicionó esa confianza y se robó algunos de nuestros secretos."[5][9] Alexander cuestiona el hecho que Snowden haya filtrado documentos secretos pero no la veracidad de los mismos.

Tras las primeras revelaciones Barak Obama, entonces presidente de Estados Unidos, dijo: "No me gustan las filtraciones porque existe un motivo para que estos programas sean clasificados"[6][10] En esta rueda de prensa, como en otras intervenciones, no puso en duda la veracidad de los documentos.

En septiembre de 2013 la presidenta de Brasil Dilma Russeff en Naciones Unidas dijo sobre los programas de vigilancia masiva de Estados

5 Traducción propia: "[Snowden] betrayed the trust and confidence we had in him. This was an individual with top secret clearance whose duty it was to administer these networks. He betrayed that confidence and stole some of our secrets"

6 Traducción propia: " I don't welcome leaks, because there's a reason why these programs are classified"

Unidos que: “Se trata de una ofensa a la legislación internacional y a los principios que deben regir entre los Estados”.[11]

Los documentos utilizados para el presente trabajo son los mismos que Snowden entregó a Greenwald y Poitras; y que ellos luego publicaron a través de diversos medios de comunicación a nivel internacional. Los mismos reflejan las capacidades que la NSA decía tener, puertas adentro, hasta el primer semestre del año 2013.

1.1 Aspectos legales

En la década de 1970 se descubrió que, desde finales de la segunda guerra mundial, la NSA recolectó comunicaciones internacionales de telégrafo. Estas interceptaciones incluyeron comunicaciones de millones de ciudadanos de Estados Unidos. Entre 1940 y 1973 la CIA y el FBI participaron en un programa encubierto para interceptar los correos dentro de Estados Unidos. Con la intención de controlar a estas agencias, en 1978 el congreso norteamericano aprobó la Ley de Vigilancia de Inteligencia Extranjera (FISA por sus siglas en inglés).[12]

Greenwald explica en su libro, “Snowden. Un Lugar sin donde Ocultarse”, que para interceptar comunicaciones de ciudadanos norteamericanos se debe tener una aprobación en la corte de FISA que:

> Se reúne totalmente en secreto, sus resoluciones son calificadas automáticamente como «secretas», y se permite asistir y exponer sus argumentos solo a una parte, el gobierno. Resulta revelador que durante años estuvo alojado en el Departamento de Justicia, lo cual dejaba descaradamente clara su función como organismo integrado en el poder ejecutivo y no como tribunal independiente con una verdadera labor supervisora… Los resultados han sido exactamente los que cabía esperar; el tribunal casi nunca rechaza solicitudes concretas de la NSA para vigilar a ciudadanos norteamericanos. Desde sus inicios, FISA ha dado el visto bueno final: en sus primeros veinticuatro años de existencia, desde 1978 a 2002, el tribunal ha rechazado un total de cero peticiones —cero— del gobierno y aprobado muchos miles. En los diez años posteriores, hasta

2012, el tribunal ha denegado solo once solicitudes gubernamentales; en conjunto, ha cursado más de veinte mil solicitudes.[6, pp. 159–160]

En 2001 seis semanas después de los atentados del once de septiembre, en Estados Unidos, se aprobó la Ley Patriota[7]. Según ACLU, la sección 215 de esta ley, permite al FBI forzar a proveedores de servicios de Internet a entregar información sobre sus clientes. Los proveedores tienen prohibido informar sobre estas acciones, incluso a los usuarios que están siendo vigilados. De esta manera sería muy difícil cuestionar una pesquisa injusta.[13]

ACLU sostiene que la Ley Patriota es inconstitucional ya que viola la primera y cuarta enmienda de la constitución de Estados Unidos. La primera enmienda garantiza la libertad de expresión. Prohibir a prestadores de servicios informar sobre vigilancia a sus usuarios sería una violación a esta enmienda. La cuarta enmienda que prohíbe realizar pesquisas sin orden judicial.

Después de los atentados de 2001 el gobierno de Bush fue responsable de incumplir la ley FISA y haber espiado ciudadanos norteamericanos sin órdenes judiciales. En el año 2008 para justificar estas actividades se reformó FISA y se añadió la sección 702. Los programas UPSTREAM y PRISM fueron justificados a través de esta sección. En el caso del último, se permite vigilar a alguien con el 51% de probabilidad de que no sea ciudadano norteamericano[8]. La EFF sostiene que la sección 702 viola la cuarta enmienda de la constitución de los Estados Unidos.[14]

El 2 de junio de 2015, el Senado de Estados de Unidos aprobó una nueva ley conocida como USA Freedom Act. Esta ley terminó con la recogida masiva de metadatos en territorio de Estados Unidos, pero continuaran almacenados por los operadores telefónicos; por lo que podrían ser solicitados. En el caso de ciudadanos de Estados Unidos hay un avance, para el resto de personas del mundo no.[15]

---

7 Conocida en inglés como *USA/PATRIOT Act*
8 Los programas PRISM y UPSTREAM son explicados en la sección 2.4.

El periodista británico Duncan Campbell,[9] en un artículo publicado en el periódico El País de España en julio de 2013, resume que la vigilancia masiva "... a no ser que uno sea ciudadano estadounidense y viva en Estados Unidos, no hay ningún límite." Campbell además llamó a los líderes de la Unión Europea a preguntarse "¿Desde cuándo los derechos humanos no son universales?" [16]

Esta pregunta deben hacerse los líderes y ciudadanos de todos los países del mundo. El artículo 12 de la Declaración Universal de los Derechos Humanos dice:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[17]

Países latinoamericanos también consideran la privacidad de las comunicaciones en sus respectivas legislaciones. En el caso de Ecuador, la no interferencia de las comunicaciones privadas esta protegida en el artículo 66 literal 21 de la constitución:

> El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.[18]

En el caso de Argentina, explica el experto en delitos informáticos Rodrigo Iglesias, la protección del correo epistolar está protegido por el artículo 18 de la constitución. La Corte Suprema de Justicia entendió al correo electrónico como epistolar y esta es la base por la que se entiende que todas las comunicaciones por Internet se encuentran protegidas.

Además el inciso 22 del artículo 75 de la constitución reconoce a diversos tratados internacionales relacionados con derechos humanos con

9 Duncan Campbell denunció en 1988 el programa de vigilancia global a través de satélites conocido como ECHELON. En el capítulo 2.5 se explican estas revelaciones y lo que se sabe ahora gracias a los documentos de Snowden.

jerarquía constitucional. Por último el artículo 19 protege el derecho a la privacidad. Iglesias sostiene que "...por lo tanto la protección legal a la privacidad está contemplado en el ordenamiento jurídico argentino y el mismo reconoce al derecho internacional que le abarca y lo hace norma fundamental del País..."[19]

Además, Iglesias explica que salvo los países que integran el consejo de seguridad de Naciones Unidas de forma permanente, los demás miembros de este organismo están obligados a proteger los derechos humanos de sus ciudadanos. Sin embargo, es poco lo que se ha hecho para proteger legalmente la privacidad de los ciudadanos de la de la vigilancia global.

En el caso de Argentina, el gobierno, quiere avanzar en la dirección opuesta. En el año 2016 anunció la cooperación con Facebook para modernizar las comunicaciones dentro del gobierno.[20] De esta forma se estaría dando acceso a información sensible del Estado a una de las empresas del programa PRISM.

Si bien no hay indicios de los avances en este proyecto, no es el único caso en que el gobierno Argentino ha querido ceder el control de las comunicaciones y la información a empresas de Estados Unidos. En 2017 anunció un acuerdo de colaboración con Amazon en el que, para su ejecución, se debe cambiar la ley de protección de datos personales.[21]

Es decir, en lugar de mejorar la protección de la privacidad de los ciudadanos porque se sabe que existen programas de vigilancia global. Se quiere flexibilizar la actual legislación para permitir que empresas extranjeras puedan guardar datos personales de ciudadanos argentinos. Amazon no aparece dentro de los documentos analizados como empresa que colabora con la NSA. Sin embargo, el uso de empresas estadounidense para espiar comunicaciones es una práctica vieja como se verá en la sección 2.2 del presente documento.

1.2 Sobre la información recolectada

La NSA recolecta datos y metadatos; los primeros son el contenido de las comunicaciones mientras que los segundos describen a ese contenido. En el caso de una llamada telefónica, por ejemplo, los datos son el audio de la conversación. Los metadatos son los números de teléfono de los participantes, la hora en que se realizó, el tiempo en que duró, etcétera.

Los metadatos son almacenados por un tiempo mayor que los datos ya que permiten tener un contexto sobre las comunicaciones y ocupan menos recursos de almacenamiento. Según Snowden:

> En la mayoría de los casos, el contenido no es tan valioso como los metadatos, ya que puedes volver a buscar contenido basado en los metadatos. Caso contrario, simplemente se puede recolectar las comunicaciones futuras que resulten de interés debido a que los metadatos te dicen que flujo de datos son los que te interesan.[10][22]

El proyecto Inmersion,[11] del Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés), permite analizar los metadatos de cuentas de algunos servicios de correo en línea; entre los que se encuentra Gmail. Luego de autorizar el análisis de la cuenta, el sistema analiza todos los correos y extrae los siguientes metadatos de cada mensaje: fecha y hora en la que se envío, remitente y destinatarios. A través de esta información genera la red de contactos de una persona como se puede ver en la imagen 1.

10 Traducción propia del inglés: " *In most cases, content isn't as valuable as metadata because you can either re-fetch content based on the metadata or, if not, simply task all future communications of interest for permanent collection since the metadata tells you what out of their data stream you actually want.*"

11 https://immersion.media.mit.edu/

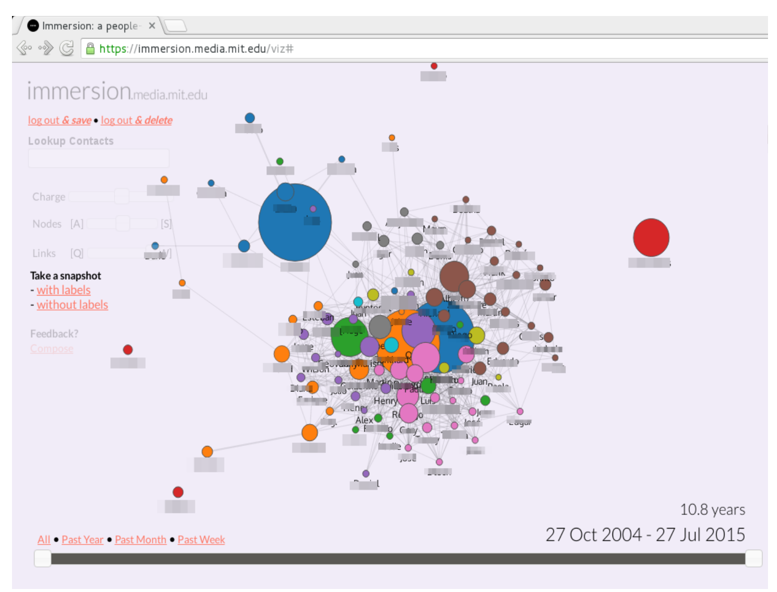


Imagen 1: Red de contactos de un usuario de Gmail
Fuente: http://immersion.media.mit.edu/

Es normal que un Estado realice vigilancia a grupos o individuos sospechosos de haber cometido algún delito. En democracias modernas este tipo de vigilancia se debe realizar a través de una orden judicial, que determine que hay indicios de que alguien es sospechoso de haber cometido un crimen.

La vigilancia masiva es cuando se espía a poblaciones enteras. Según la organización Privacy International la vigilancia masiva es:

> ... la sujeción de una población o componente significativo de un grupo al monitoreo indiscriminado. Implica una interferencia sistemática con el derecho de las personas a la privacidad.(…) Cualquier sistema que genere y recopile datos sobre individuos sin intentar limitar el conjunto de datos a personas definidas como objetivos de vigilancia es una forma de vigilancia masiva.[12] [23]

12 Traducción propia. “*Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. ... Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance.*”

En la imagen 2 se puede ver una diapositiva, del archivo de Snowden, que muestra las características de vigilancia masiva que tienen los programas de la NSA. En la misma se puede ver las intenciones de la agencia para "oler" todo, saber todo, recoger todo, procesar todo, explotar todo y colaborar con otras agencias. "¡Bienvenidos al Imperio de la Vigilancia!"[15, p. 20]

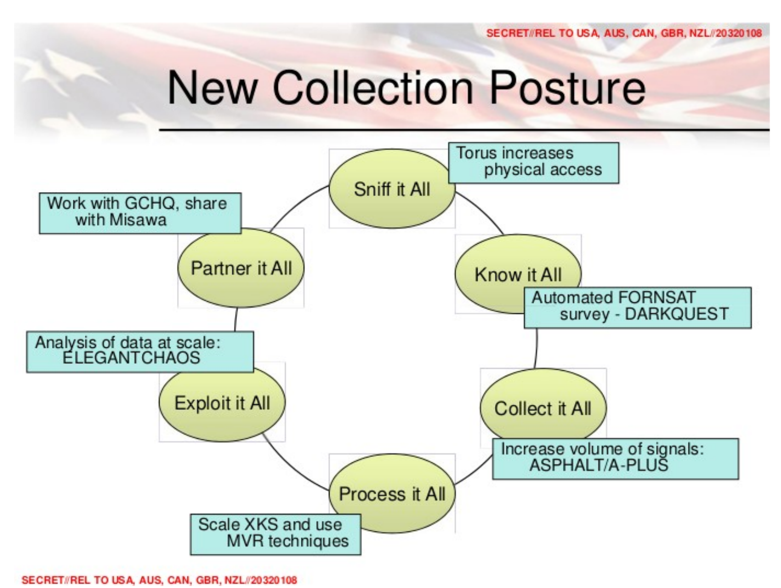


Imagen 2: Recolectarlo todo
Fuente: https://edwardsnowden.com

2 Recolección de información

La herramienta "Informante sin Límites" provee, a la NSA, la capacidad de saber cuánta información y desde donde está siendo recolectada.[24] Este sistema, a través de un mapa interactivo, permite visualizar la cantidad de comunicación telefónica (DNR) y de Internet (DNI) es recolectada. En la imagen 3 se puede ver una captura de pantalla de dicha herramienta.[25]

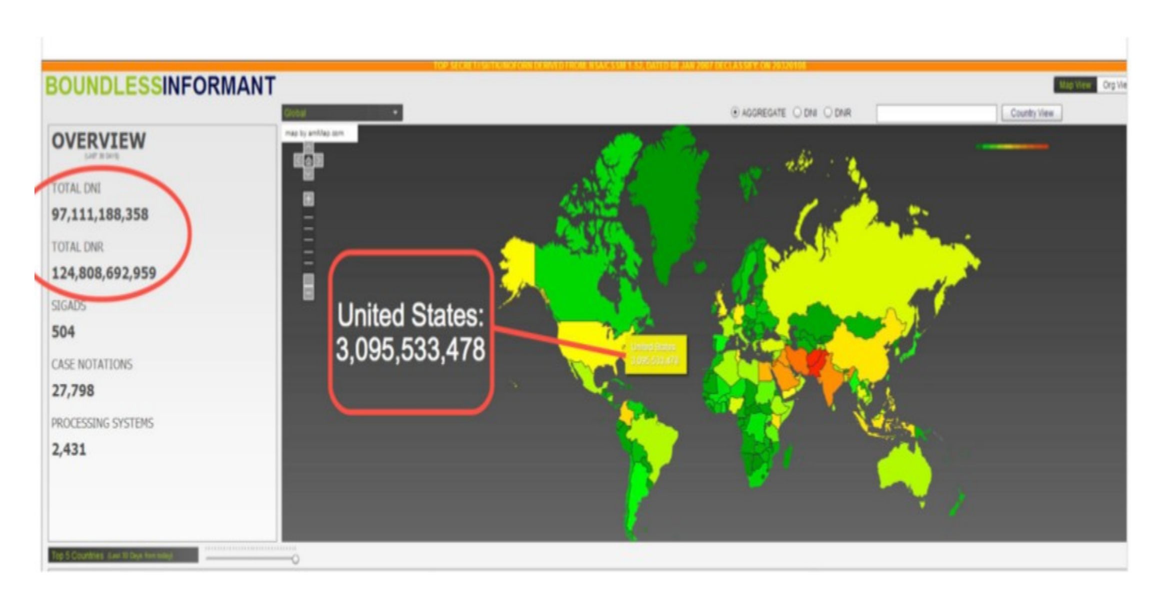


Imagen 3: Mapa interactivo del programa Informante sin Límites
Fuente: https://edwardsnowen.com

Greenwald detalla el alcance de la vigilancia en su libro:

> En conjunto, en solo treinta días la unidad había recogido datos de más 97 mil millones de e-mails y 124 mil millones de llamadas telefónicas de todo el mundo. Otro documento «INFORMANTE SIN LÍMITES» detallaba los datos internacionales recopilados a lo largo de un período de treinta días en Alemania (500 millones), Brasil (2.300 millones) y la India (13.500 millones). Y aun otros archivos mostraban recogida de metadatos en colaboración con los gobiernos de Francia (70 millones), España (60 millones), Italia (47 millones), Holanda (1,8 millones), Noruega (33 millones) y Dinamarca (23 millones).[6, p. 116]

Estas comunicaciones son recolectadas por la NSA de diversas maneras. En la imagen 4 se puede ver una diapositiva, de una presentación

de máximo secreto, donde se explica que la NSA tiene cinco formas de recolectar datos: 3rd PARTY/LIAISON, REGIONAL, CNE, LARGE CABLE y FORNSAT. [26]

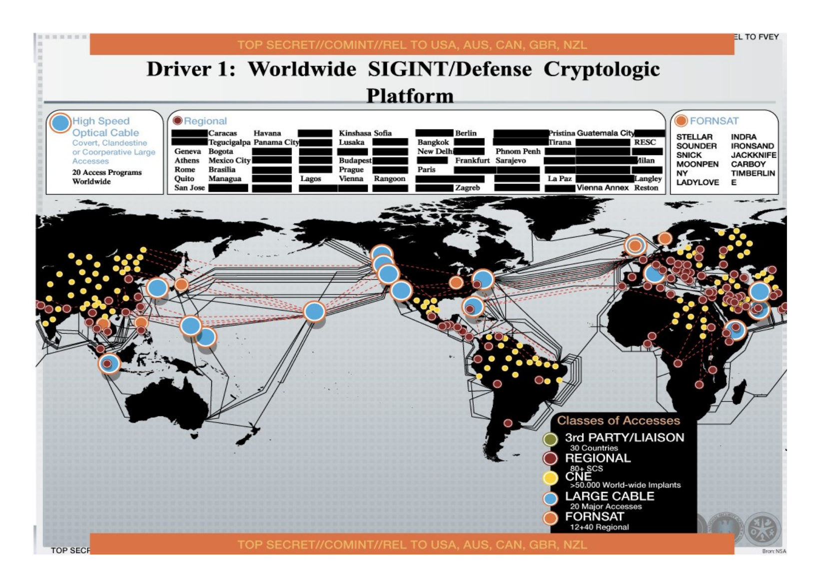


Imagen 4: Mapa global de recolección de información

Basado en este, y otros documentos, el portal Electrospaces.net realizó un análisis para explicar las formas en que la NSA puede acceder a la información. El programa 3rd PARTY/LIAISON se basa en la colaboración de la NSA con agencias de inteligencia de otros países. REGIONAL consiste en el espionaje que realiza la agencia en embajadas y consulados alrededor del mundo. CNE consiste en ataques a redes de computadoras realizadas por la unidad conocida como TAO. El programa LARGE CABLE es el que se encarga de recolectar la información en colaboración con empresas de comunicaciones. Por el último, FORNSAT se encarga de las comunicaciones satelitales.[27]

2.1 Recolección a través de empresas tecnológicas

La NSA es una institución pública donde trabajan aproximadamente treinta mil personas de forma directa. Sin embargo, alrededor de sesenta mil lo hacen a través de contratistas privados. Cuando Snowden trabajó para Dell o Booz Allen Hamilton, en realidad lo hizo para la NSA. Incluso lo hacía desde las oficinas de la NSA teniendo acceso a sus secretos.[6]

El nombre de las empresas que trabajan con la NSA es un secreto resguardado por la agencia. Incluso en los documentos de Snowden se menciona solo unas pocas. En la imagen 5 se puede ver una diapositiva que muestra algunas de ellas y las áreas en las que operan.[28]



Imagen 5: Empresas que colaboran con la NSA
https://edwardsnowden.com

La unidad de Operaciones de Fuentes Especiales (SSO por sus siglas en inglés) se encarga de manejar las relaciones entre la NSA y las corporaciones tecnológicas. Existen, por lo menos, dos formas en las que recolecta información con estas empresas. La primera conocida como PRISM donde participan empresas que proveen servicios en Internet. La segunda se la conoce como UPSTREAM y se recolecta la información a través de las empresas que manejan los cables de fibra óptica como se puede ver en la imagen 6 [29]



Imagen 6: PRISM y UPSTREAM
Fuente: https://edwardsnowden.com

2.1.1 UPSTREAM: empresas de telecomunicaciones

Gran parte de la infraestructura de comunicaciones está implementada con tecnología de empresas estadounidenses, lo que representa una ventaja estratégica para este país. Históricamente los Estados Unidos ha sabido utilizar esta ventaja a su favor.

En el año 1959 la NSA espió al gobierno de Fidel Castro, en Cuba, gracias a que la red de telefonía estaba implementada con la tecnología de la empresa RCA. Esta empresa colaboró con la agencia para esta operación. Incluso en el año 1945, la Agencia de Seguridad del Ejército,[13] en conjunto que las empresas de telecomunicaciones, espiaron los mensajes internacionales de telégrafo que pasaban por suelo estadounidense. [1]

En la actualidad no son los cables de telégrafo los que transmiten las comunicaciones a través de Estados Unidos. Son los cables de fibra óptica, con las comunicaciones de Internet, los que atraviesan este país. En el caso de América Latina, casi todas las comunicaciones viajan a otras partes del mundo a través de Estados Unidos como se puede ver en la imagen 7.[30]

13 Agencia que precedió a la NSA.



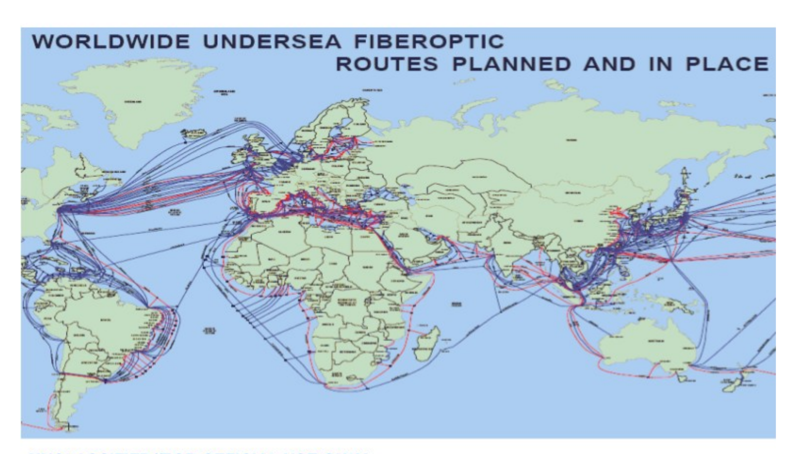


Imagen 7: Mapa mundial de cables de fibra óptica

Los documentos de Snowden no nombran a las empresas que participan en la recolección de datos a través de cables de fibra óptica. En su lugar, utilizan códigos que describen a los programas que manejan la relación con las empresas. Algunos de los nombres revelados son: BLARNEY, FAIRVIEW y STORMBREW.

En el año 2015, The New York times realizó una investigación donde comparó información de los documentos de Snowden con noticias públicas. A través de la misma, logró determinar que el programa FAIRVIEW se refiere a AT&T, mientras que STORMBREW se refiere al trabajo realizado con la empresa Verizon. [31]

La NSA aprovecha el poder estratégico de las redes de fibra óptica, operada por empresas norteamericanas.[32] The New York Times, explica que el trabajo entre la NSA y las empresas de comunicaciones se realiza en buenos términos. En el año 2006 ya se hablaba de la existencia de un cuarto secreto dentro de las oficinas AT&T en San Francisco donde operaba la NSA.[31]

Independientemente de la forma en que la NSA trabaje con estas empresas, puede recurrir a presiones legales. Este fue el caso que sucedió en 2013 cuando obligó a Verizon a recolectar metadatos de las comunicaciones de millones de usuarios dentro de Estados Unidos.[4]

Luego de las revelaciones de Snowden ha existido ciertos cambios legales que dan más control sobre las capacidades de recolección de datos por parte de agencias de inteligencia.[33] Sin embargo la vigilancia sobre ciudadanos no estadounidense sigue sin ningún tipo de protección legal.

2.1.2 PRISM: empresas de Internet

Una presentación digital sobre el programa PRISM dice que es la herramienta de recolección de información más utilizada por la NSA para generar reportes. El programa consiste en el trabajo que realiza la NSA y el FBI para acceder a información de los usuarios de empresas como: Microsoft, Google, Yahoo, Facebook, Youtube,[14] Skype[15] y Apple como se puede ver en la imagen 8. Para el primer semestre de 2013 se anunció que pronto se sumaría el servicio de Dropbox.

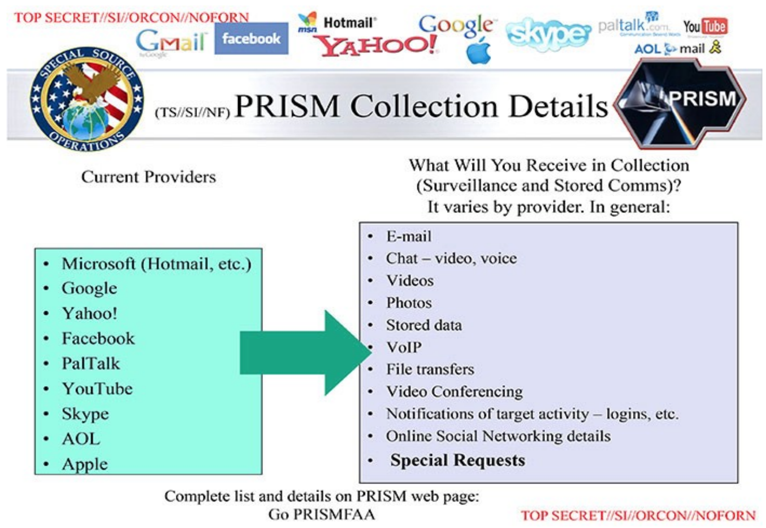


Imagen 8: Empresas que participan en PRISM
Fuente: https://edwardsnowden.com

Estas empresas proveen acceso a la NSA de los datos de los usuarios que utilizan sus servicios. Información como: correo electrónicos, chats, videos, información almacenada, voz sobre IP, transferencia de archivos, video conferencias, notificación de actividad de un objetivo de vigilancia como acceso a una cuenta, detalles de la actividad en redes sociales y solicitudes especiales.

14 Youtube fue comprado por Google en 2006.
15 Skype fue comprado por Microsoft en 2011.

A diferencia de otros programas de recolección como FAIRVIEW o STORMBRIEW, en PRISM la NSA no recolecta la información de todos los usuarios todo el tiempo. La información está almacenada en los servidores de estas empresas y es almacenada por los usuarios al usar estos servicios.

Sucede que la nube no existe y la información se almacena en los servidores de las empresas que proveen los servicios. Si se utiliza el servicio de Gmail, por ejemplo, los correos electrónicos se almacenan en los servidores de Google. Cuando se comparte un archivo a través de Dropbox, el archivo se lo comparte a Dropbox. Así con todas las demás empresas que proveen este tipo de servicios en Internet.

Incluso si los usuarios borran archivos de los servidores, no hay garantía que los mismos desaparezcan. En enero del 2017 se descubrió un error en el servicio de Dropbox en que archivos eliminados, por sus usuarios, volvieron a aparecer. En algunos caso llegaron a aparecer archivos eliminados siete años atrás. [34]

Ramonet explica que "Con el impulso del consumo 'en línea' se ha desarrollado considerablemente la vigilancia de tipo comercial que ha generado un gigantesco mercado de datos personales, convertidos en mercancía."[15, pp. 14–15] Continúa más adelante "Facebook o Google, por ejemplo, no venden nada a los internautas; venden sus miles de millones de usuarios a los anunciantes publicitarios."[15, p. 20]

Esto resulta conveniente para la NSA que cuando quiere vigilar a alguien, la información ya fue recolectada. Tan solo deben seguir un procedimiento y tendrán acceso a años de información de una persona. A diferencia de sistemas como XKEYSCORE.[16] donde la información está disponible por poco tiempo, las empresas de PRISM la almacenan de forma indefinida. ¿Alguna vez buscó un correo electrónico de hace varios años en uno de estos sistemas y lo encontró?

16 XKEYSCORE es un sistema de análisis de información que se explica en detalle en el capítulo 3.

El blog Electrospaces.net[17] realizó un análisis sobre los documentos de PRISM. Según el mismo, existen dos formas de acceder a la información. La primera se realiza sobre la información que se encuentra almacenada y se la conoce como *Stored Comms.* La segunda es la que se realiza desde el momento que se autoriza el seguimiento a una persona y se la conoce como vigilancia (*Surveillance)*. Existe discrepancia sobre si la capacidad de vigilancia permite vigilar en tiempo real o no. Según Electrospaces.net no existe evidencia de que se espíe en tiempo real.[35]

Los diarios que publicaron los documentos de PRISM sostienen que se puede realizar vigilancia en tiempo real. The Guardian sostiene que: *"…la NSA tiene la capacidad de acceder directamente a los servidores de las compañías participantes y obtener, comunicaciones almacenadas así como realizar recolección de datos en tiempo real sobre las comunicaciones de los usuarios [objetivos de vigilancia] "*[18].[36] The Washington Post dice que: *"El formato de codificación de PRISM refleja la capacidad, confirmada por reportes de The [Washington] Post de la capacidad de vigilancia en tiempo real así como de contenidos almacenados""*[19][37]

En la imagen 9 se ve la diapositiva a la que The Washington Post hace referencia. En la misma se ve el código P2ESQC120001234. Según este medio la letra "C" (RTN-EDC) quiere decir que se va a recibir notificaciones en tiempo real de eventos como ingreso a la cuenta de correo o envío de un correo. La letra D (RTN-IM) sirve para notificar en tiempo real actividad relacionada con mensajería instantánea como ingreso[20] o la salida[21] de un usuario de una cuenta de chat.

17 https://electrospaces.blogspot.com.ar
18 Traducción propia: *"… the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users."*
19 Traducción propia: "The PRISM case notation format reflects the availability, confirmed by The Post's reporting, of real-time surveillance as well as stored content."
20 *Login*
21 *Logout*

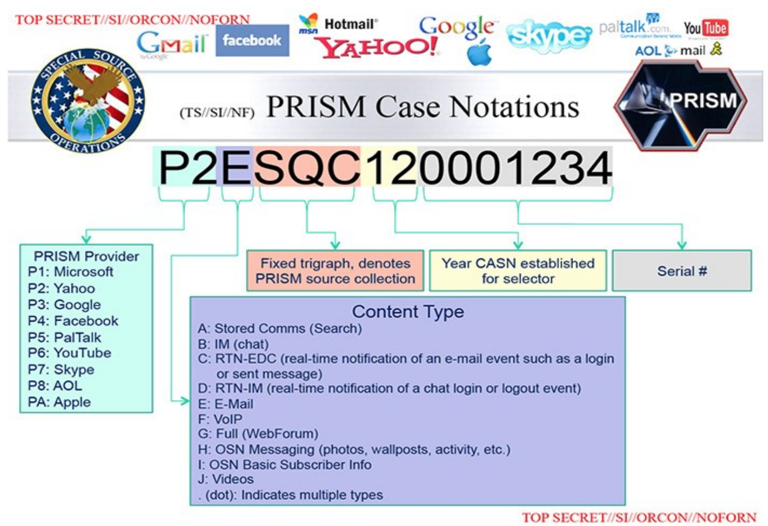


Imagen 9: Codificación de PRISM muestra acceso tiempo real
Fuente: https://edwardsnowden.com

Independientemente de si la información se puede recolectar en tiempo real o no, queda claro que cualquier información que alguien almacene en estos servicios podría ser accedida por estas empresas o el gobierno de los Estados Unidos algún momento en el futuro.

Recolección de la información

Al estar las empresas de PRISM dentro de los Estados Unidos es el FBI el que accede a la información por tratarse de vigilancia doméstica. En la imagen 10 se puede ver otra diapositiva, de la presentación sobre PRISM, en la que se explica el procedimiento que debe seguir un analista de la NSA para acceder a la información de una persona.

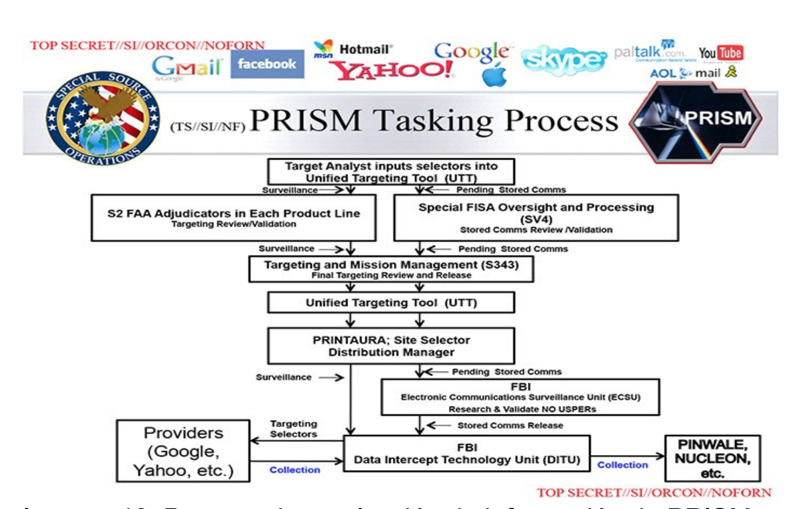


Imagen 10: Proceso de recolección de información de PRISM
Fuente: https://edwardsnowden.com

A través del aplicativo “Herramienta Unificada para Vigilancia” (UTT por sus siglas en inglés[22]) se solicita el acceso a los datos de alguien. Dependiendo si la vigilancia va a ser de tipo *Stored Comms o Surveillance* la solicitud debe ser autorizada justificando que existe una probabilidad de al menos el 51% de que la persona a ser vigilada no es un ciudadano de Estados Unidos y que se encuentra fuera de ese país. En el caso de *Stored Comms* se hace una validación adicional por parte del FBI para asegurarse la persona a ser vigilada no sea estadounidense. [37]

Al finalizar el proceso de recolección la información es proporcionada por las empresas y esta ingresa a varios sistemas de la NSA para su análisis como se verá en la sección 3.2 del presente trabajo.

Si bien los ciudadanos de Estados Unidos tienen cierta protección legal, queda claro que para el resto de personas del mundo este no es así.

Cooperación de PRISM con la NSA y el FBI

Como se pudo ver, la NSA trabaja conjuntamente con el FBI para acceder a la información almacenada en los servidores de las empresas. Históricamente, la NSA ha recolectado información para otras agencias de Inteligencia dentro de los Estados Unidos, en especial la CIA.[1] En un memo interno de 2012 se dice sobre el trabajo entre la NSA, la CIA y el FBI: “¡Estas dos actividades ponen en relieve la cuestión de que PRISM es un deporte en equipo!”[6, p. 145]

2.1.3 Trabajo empresas con la NSA

Las diapositivas de PRISM dicen que la información se recolecta directamente desde los servidores de las empresas. Chris Gaither, entonces vocero de Google, en entrevista realizada por la revista Wired, afirmó que la forma en la que Google entrega la información es a través de SFTP,[23] y en ocasiones directamente en persona.[38]

22 Unified Surveillance Tool
23 Protocolo cifrado para intercambio de archivos.

The New York Times, poco tiempo después de las filtraciones de PRISM publicó un artículo en el que afirmó que Google y Facebook proveían al FBI la información a través de un portal seguro. La fuente de esta noticia eran empleados no identificados de las dos empresas.[39]

Si bien los reportes de la revista Wired rinde su versión una fuente oficial de Google y en los reportes de The New York Times se cita a fuentes anónimas de Google y Facebook. En ninguno de los dos casos se citan documentos que sustenten estas afirmaciones. En el caso de Microsoft existe documentos que detallan algunos ejemplos de la forma en la que esta empresa colaboró con el gobierno de Estados Unidos.

En el año 2012 el portal Outlook.com de Microsoft añadió la funcionalidad de cifrado en sus *chats*. Esto preocupó a la NSA porque no podría espiar las comunicaciones de este portal. Según memorando interno de SSO, del 26 de diciembre de 2012 el problema se solucionó gracias a que "MS [Microsoft], en colaboración con el FBI, desarrolló una capacidad de vigilancia para hacer frente a la nueva SSL[24]." [6, p. 144]

El servicio Skydrive de Microsoft[25] permitía compartir archivos a través de Internet. Desde el 7 de marzo de 2013, PRISM pudo recolectar las comunicaciones almacenadas por este servicio. Según un documento interno de SSO: "Este éxito resulta de los muchos meses de colaboración del FBI con Microsoft..."[6, p. 141]

Los documentos también hablan sobre el trabajo realizado por Microsoft para mejor la capacidad de vigilancia en Skype. Cuando The Guardian realizó estas denuncias el doce de julio de 2013 pidió la posición de Microsoft al respecto. Ellos mencionan que la empresa está comprometida a entregar información solo a cuando la ley le obliga. En el último punto de su comunicado dicen:

> Finalmente, cuando actualizamos nuestros productos las obligaciones legales podrían, en algunas circunstancias, requerir que mantengamos la habilidad de proveer información en respuesta a solicitudes relacionadas

24 SSL es un protocolo que permite asegurar las comunicaciones en Internet.
25 El servicio ahora se llama OneDrive.

con seguridad nacional. Existen aspectos de este debate que deseamos que estuviéramos en la posibilidad de discutir con mayor libertad[26] [40]

Es probable que las otras compañías trabajen de forma similar dentro del programa PRISM. El funcionamiento técnico no es claro, sin embargo estas empresas tienen obligación legal de proporcionar la información al gobierno de Estados Unidos.

La historia de colaboración entre el gobierno de Estados Unidos y las corporaciones no se limita a las empresas de PRISM. AT&T tiene una historia de varias décadas en las que se sabe que colaboró con la NSA. En 1985 la NSA inició el programa FAIRVIEW en conjunto con AT&T. Ese mismo año AT&T tuvo un contrato de mil millones de dólares para proveer computadoras y servicios de Internet para la NSA. En 2001 la NSA creo el programa de vigilancia Stellar Wind del cuál AT&T fue la primera en sumarse. En 2006 Mark Klein, ex empleado de AT&T, denunció la existencia de un cuarto secreto donde operaba la NSA dentro de las oficinas de San Francisco.[41]

AT&T tiene un edificio ubicado en el corazón de Manhattan, que diferencia del resto, no tiene luces ni ventanas. En su interior no contiene oficinas, sino que es uno de los nodos más importantes por donde se encuentra el corazón de la red de la empresa.

The Intercept en colaboración con Field of Vision[27] denunciaron que dentro de este edificio, la NSA y el FBI tienen el centro de operaciones conocido como TITANPOINTE. Se le mostró los documentos de esta investigación a Mark Klein, quién afirmó no estar sorprendido puesto que es un lugar lógico para realizar vigilancia.[42]

---

26 Traducción propia: *“Finally when we upgrade or update products legal obligations may in some circumstances require that we maintain the ability to provide information in response to a law enforcement or national security request. There are aspects of this debate that we wish we were able to discuss more freely.”*

27 Productora de documentales donde participa Laura Potras: https://fieldofvision.org/

2.2 Recolección con ayuda de otros países

La NSA trabaja de manera coordinada con otros países para recolectar información. La colaboración más estrecha se la realiza con los países miembros de la Alianza de los Cinco Ojos.

2.2.1 Alianza de los Cinco Ojos

El 1946 las organizaciones de inteligencia de Estados Unidos y Reino Unido[28] firmaron el acuerdo de colaboración para compartir información. En 1953 el acuerdo conocido como UKUSA fue actualizado con la participación adicional de Canadá, Nueva Zelanda y Australia.[43]

Este acuerdo de colaboración entre agencias de inteligencia se conoce, hoy en día, como La Alianza de los Cincos Ojos. Según el periodista británico Duncan Campbell: “La organización multinacional de escuchas UKUSA, creada por varios tratados secretos de posguerra entre Estados Unidos y Gran Bretaña, se llama hoy a sí misma los Cinco Ojos. ”[16]

La Alianza de los Cincos Ojos está conformada por la NSA de Estados Unidos, GCHQ de Inglaterra, CSEC de Canadá, GCSB de Nueva Zelanda y ASD de Australia. Gran parte de documentos de máximo secreto se comparten con estos países bajo la codificación FVEY[29].

La relación de la NSA con estos países es de cooperación y trabajan juntos para recolectar información. Por ejemplo, CSEC trabajó en conjunto con la NSA para espiar al ministerio de Petróleos de Brasil. No se espían entre si, salvo que una agencia solicite a la otra recolectar información. La NSA podría espiar a ciudadanos británicos para la GCHQ y viceversa.[6]

Reino Unido y GCHQ

The Guardian publicó un reportaje que muestra las capacidades de vigilancia de Reino Unido y su colaboración con la NSA. En el mismo detalla que dos de los principales programas en los que trabaja la GCHQ se

28 En ese entonces todavía no existía la NSA.
29 Abreviado de Five Eyes o Cinco Ojos en español.

conocen como Dominar el Internet[30] y Explotación Global de las Telecomunicaciones[31]. Los mismos buscan recolectar la mayor cantidad de comunicaciones de Internet y telefónicas posibles.[44]

El programa TEMPORA se encarga de interceptar las comunicaciones que viajan a través de los cables de fibra óptica. Reino Unido se encuentra en un lugar privilegiado por donde atraviesan cables que unen a Europa con América. Además la GCHQ tiene la ventaja de que Gran Bretaña tiene menos controles legales, que Estados Unidos, para limitar la vigilancia.

La GCHQ utiliza un *wiki*[32] interno para la documentación de sus herramientas. En él, se afirma que TEMPORA tiene la capacidad de interceptar tráfico de Internet para almacenar contenido de comunicaciones por tres días y metadatos por treinta días. La información incluye tráfico de navegación, chat, correo, voz/IP, entre otros. Dicen que el sistema es agnóstico por lo que se puede ser utilizado por otras aplicaciones, como XKEYSCORE, para su análisis.[45]

La GCHQ recolecta la información a través de empresas proveedores de servicios de telecomunicaciones[33], de manera similar a como opera la NSA. Entre las empresas que han trabajado con la agencia se encuentran Verizon, BT y Vodafone[34]. En los documentos de Snowden hay archivos con el nombre clave de GERONTIC que hacen referencia a la empresa Cable & Wireless. Esta fue adquirida por Vodafone en el año 2012. [46]

The Guardian cita un documento[47] de la GCHQ donde dice que Reino Unido es el país con mayor acceso a las comunicaciones de Internet dentro de la Alianza de los Cinco Ojos. Este poder es compartido con la NSA, según otro documento[45] en mayo de 2012 eran 250 los analistas de

30 Traducción propia del inglés: “Mastering the Internet”.
31 Traducción propia del inglés: “Global Telecoms Exploitation”.
32 Herramienta utilizada para construir comunicación de forma colaborativa. El wiki más conocido es la enciclopedia en línea Wikipedia.
33 Ver sección 2.1.1
34 Vodafone es una de las empresas de telecomunicaciones con más usuarios en el mundo.

la NSA y 300 de la GCHQ que tenían acceso a la información recolectada por TEMPORA.[48]

2.2.2 Otros países

El segundo nivel de colaboración, luego del de la Alianza de los Cinco Ojos, se los conoce como grado B o terceros. Estos son países con los que la NSA trabaja en conjunto para recolectar información. En la imagen 11 se puede ver un documento de 2013 que muestra un listado de los países y organizaciones con los que la NSA comparte información.[49]



Imagen 11: Países con los que la NSA comparte información
Fuente: http://glenngreenwald.net/

El último peldaño son los países que son espiados por los Estados Unidos, pero con los que nunca comparte información. En esta lista se encuentran adversarios conocidos como China, Rusia, Irán, Venezuela y Siria; pero también países como Brasil, México o Argentina.[6]

2.3 Recolección en embajadas y consulados

En octubre de 2013 el semanario alemán Der Spiegel publicó un artículo titulado “El Nodo secreto de Espionaje de la NSA en Berlín.”[35][50] En el mismo explica como las embajadas son utilizadas para recolectar información de las redes de telefonía celular. El trabajo de espionaje lo

35 Traducción propia del inglés: “The NSA's Secret Spy Hub in Berlin”

realiza una unidad conformada por agentes de la NSA y la CIA conocida como “Servicio Especial de Recolección” (*SCS* por sus siglas en inglés).

Los agentes de SCS operan como miembros diplomáticos de las delegaciones de Estados Unidos en embajadas y consulados alrededor del mundo. En el caso de Alemania tienen centros de operaciones en Berlín y Fráncfort. El diario Italiano l'Espresso realizó otra investigación y menciona que en el caso de Italia SCS trabaja en las ciudades de Roma y Milán.[51]

Un extracto de una presentación de la NSA dice que para enero de 2002 existían 65 localidades donde operaban equipos SCS. En la imagen 12 se puede ver que en 2002 la CIA y la NSA mantenían equipos de espionaje en embajadas y consulados de ciudades alrededor del mundo. En el caso de Iberoamérica están listadas ciudades como: La Paz, Quito, Bogotá, Basilia, Caracas, Ciudad de Guatemala, Madrid, México DF y Tegucigalpa.[52]



Imagen 12: Mapa de localidades SCS alrededor del mundo
Fuente: https://edwardsowden.com

Tanto Der Spiegel como l'Espresso mencionan el uso de paneles dialéctricos en las paredes superiores de las embajadas con forma de ventanas para esconder antenas. Estas antenas serían utilizadas para interceptar señales de comunicaciones inalámbricas como las redes telefonía móvil.

Jacob Appelbaum, quién participó en la investigación de Der Spiegel, estuvo en Quito a finales del 2013 para participar en el evento Minga por la

Libertad[36]. Aprovechó el viaje para constatar si la Embajada de Estados Unidos en Quito tenía paneles dialéctricos similares a los de Berlín. Según lo que pudo ver afirmó que los paneles existen y que la embajada está ubicada estratégicamente para poder interceptar las comunicaciones de la ciudad. [53]

El uso de misiones diplomáticas para realizar espionaje de las ondas de telecomunicaciones se lo practicaba en la guerra fría. Según Aid, en los años 1960s la embajada de Estados Unidos en Moscú se utilizó para interceptar las comunicaciones de radio de las agencias rusas de inteligencia, la policía y miembros del gobierno. [1]

2.4 Recolección a través de satélites

Duncan Campbell es un periodista británico que 1976 hizo pública la existencia de la agencia GCHQ.[54] En agosto de 1988 reveló un programa de espionaje masivo a nivel mundial conocido como ECHELON. El mismo consistía en la interceptación de comunicaciones satelitales por parte de la NSA y GCHQ. En ese entonces ya se utilizaba computadoras para procesar grandes cantidades de datos y poder filtrar información relevante.[55]

En el año 2001 el Parlamento Europeo publicó un informe donde se confirmó la existencia de ECHELON. El mismo se realizó verificando la evidencia física de estaciones para vigilar satélites, material desclasificado, el testimonio de empleados de las agencias de inteligencias, y las versiones de los periodistas Duncan Campbell y Nicky Hager.[56]

El 5 de septiembre de 2001 el Parlamento Europeo determinó un mandato en contra de la vigilancia masiva. Lamentablemente seis días después ocurrieron los atentados del once de septiembre de 2001 y con eso se vio frustrado cualquier plan de limitar la vigilancia masiva.[57]

Según Campbell los documentos de Snowden confirman la existencia de ECHELON bajo el nombre FORNSAT.[58] El funcionamiento

36 Este evento fue organizado en la ciudad de Quito por el autor de este trabajo, quien contactó a Appelbaum para su concurrencia. Estuvo motivado en las revelaciones surgidas en el caso Snowden.

de FORNSAT consiste en estaciones terrestres que interceptan las comunicaciones satelitales. A diferencia de las antenas parabólicas que apuntan a un satélite, las antenas de estas estaciones son esféricas para conectarse con varios satélites simultáneamente. La estación de Menwith Hill está ubicada en Reino unido y es la que más información recolecta. En la imagen 13 se puede ver una foto la estación y sus antenas esféricas.[59]



Imagen 13: Fotografía de Menwith Hill
Fuente: https://theintercept.com

Para tener un alcance global, las estaciones de interceptación están distribuidas alrededor del mundo. En la imagen 14 se puede ver un mapa con la ubicación de las mismas.[60]

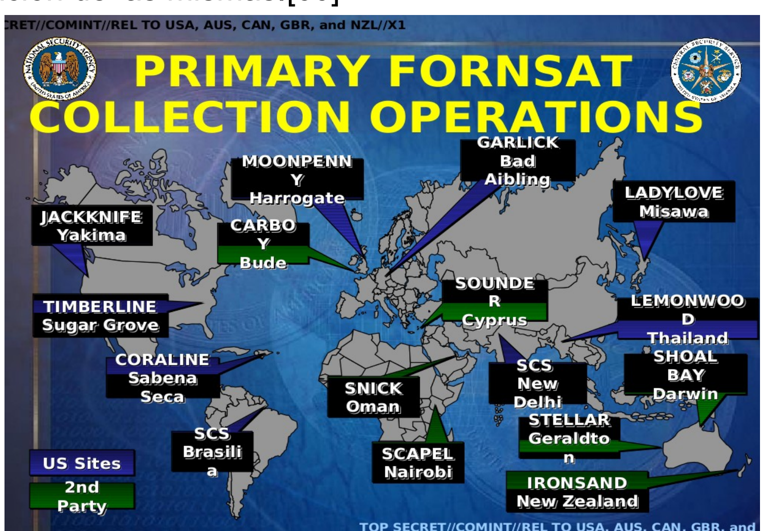


Imagen 14: Mapa de estaciones de FORNSAT
Fuente: https://edwardsnowden.com

Si bien en la actualidad la mayoría de información fluye a través de cables de fibra óptica y muy poco se lo hace por satélites. La comunicación satelital sigue siendo utilizada en zonas donde no es posible llegar con cables.

2.5 Recolección a través de ataques informáticos

La NSA puede acceder a gran parte del tráfico de Internet trabajando con corporaciones, en colaboración con agencias de inteligencia de otros países, desde sedes diplomáticas o espiando comunicaciones satelitales. Sin embargo, no puede acceder a todas las comunicaciones. Cuando hay información valiosa que la agencia desea acceder recurre a los ataques informáticos.

La unidad de Operaciones de Acceso Personalizado (TAO por sus siglas en Inglés[37]) es la que se encarga de la explotación de redes informáticas alrededor del mundo. Se creó en 1997 y actualmente es la unidad más grande de la NSA. Para 2013 se estimaba que trabajaban mil personas entre civiles y militares.[61] En la mitad de la década de 2000 TAO tuvo 258 ataques exitosos en 89 países, en 2010 realizo 279 operaciones a nivel mundial.[62]

TAO prefiere atacar redes que a individuos porque de esta manera tienen la posibilidad de acceder a más información.[63] Un objetivo importante son los sistemas que administran los cables submarinos de fibra óptica que no son controlados por la NSA. La agencia atacó los sistemas informáticos de las empresas France Telecom (hoy Orange) y Telecom Italia Sparkle. Estas empresas administran el cable submarino SEA-ME-WE-4 que conecta a Europa con el norte de África, los países del Golfo Pérsico, las costas de India, Malasia y Tailandia.[64]

Como se vio en el caso de PRISM la NSA puede solicitar información a empresas como Google, Yahoo o Microsoft. Esta no es la única forma en la que la NSA puede acceder a la información almacenada en los servidores de estas empresas. Según una investigación realizada por The Washington Post, la NSA obtuvo acceso a las comunicaciones internas de Google y Yahoo a través del programa MUSCULAR.[65] Poco tiempo después, el mismo diario, publicó otra investigación en la que se confirmó

37 *Tailored Access Operations*

que Microsoft también estaría entre las empresas norteamericanas que fueron atacadas por la NSA.[66]

Corporaciones como las antes mencionadas mantienen la información de sus servicios en varios centros de datos alrededor del mundo. Según sus necesidades mueven la información entre ellos. Para esto Yahoo y Google tienen sus propios enlaces de comunicación que conectan sus centros de datos en distintos continentes. En el caso de Google, realizó un esfuerzo importante en cifrar las comunicaciones entre sus servicios y sus usuarios. Sin embargo asumió que la información que viajaba dentro de su red interna estaba segura ya que el canal de fibra óptica era utilizado únicamente por esta empresa.

La NSA vio esta falla de seguridad como una oportunidad para acceder a información. En la imagen 15 se ve una diapositiva donde la NSA explica esta vulnerabilidad. En la nube de la izquierda están los servicios que Google publica hacia Internet donde la comunicación es cifrada. La nube de la derecha es la red interna de Google donde la comunicación no estaba cifrada.[67]

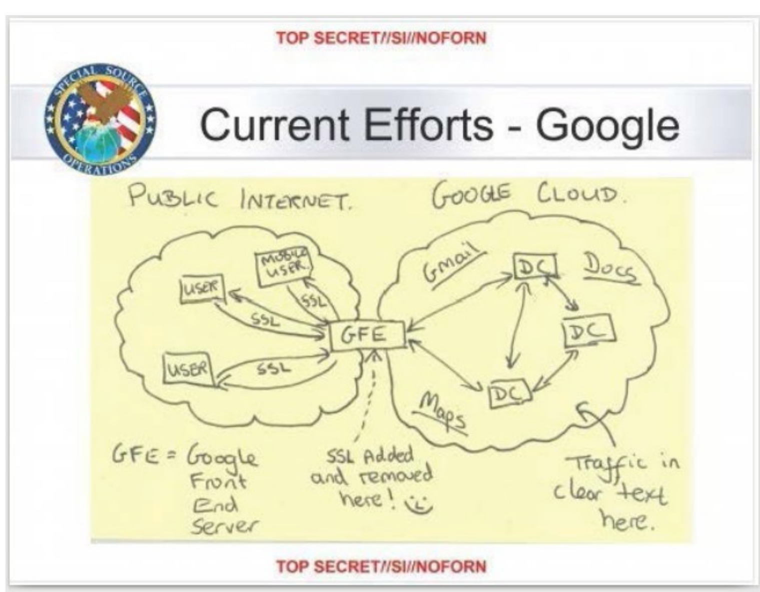


Imagen 15: Acceso de la NSA a la red de Google
Fuente: https://www.washingtonpost.com

Los proveedores de Internet son objetivos de interés para la NSA por la concentración de tráfico que fluye por su infraestructura. Der Spiegel

realizó una investigación basadas en documentos filtrados por Snowden.[68] En la misma, se puede ver que la NSA atacó a proveedores que forman parte de la infraestructura principal de Internet[38] como la empresa alemana Telekom. También atacó a empresas más pequeñas, del mismo país, como Stellar, CETEL y IABG.[69]

TAO desarrolla sus propias herramientas de software y hardware para crear puertas traseras y poder ingresar a las redes de su interés. Si bien gran parte del desarrollo se lo hace casa adentro, para el año 2013 había presupuestado 25.1 millones de dólares para la compra de vulnerabilidades a proveedores privados de programas maliciosos.[63]

ANT es la división de TAO que desarrolla herramientas de software y de hardware para realizar ataques informáticos. Tienen implantes para diversos tipos de productos informáticos. Equipos de redes de marcas Cisco, Juniper o Huawei pueden ser vulnerados permitiendo así a la NSA acceder a la información que fluye a través de los mismos. Puertas traseras que se instalan en los sistemas BIOS de computadoras y servidores que no podrían ser detectadas por los sistemas operativos. Equipos para interceptar comunicaciones celulares o de *wifi*. Son algunos de los ejemplos de las herramientas disponibles para ataques informáticos.[70]

Uno de los documentos más importantes revelados sobre ANT es un catalogo de cincuenta páginas donde se muestran las herramientas disponibles. En la imagen 16 se puede ver la explicación gráfica del funcionamiento de uno de los productos. El implante se llama JETPLOW y está diseñado para equipos Cisco de las series PIX y ASA.[71]

38 Lo que se suele conocer como *backbone* de Internet.

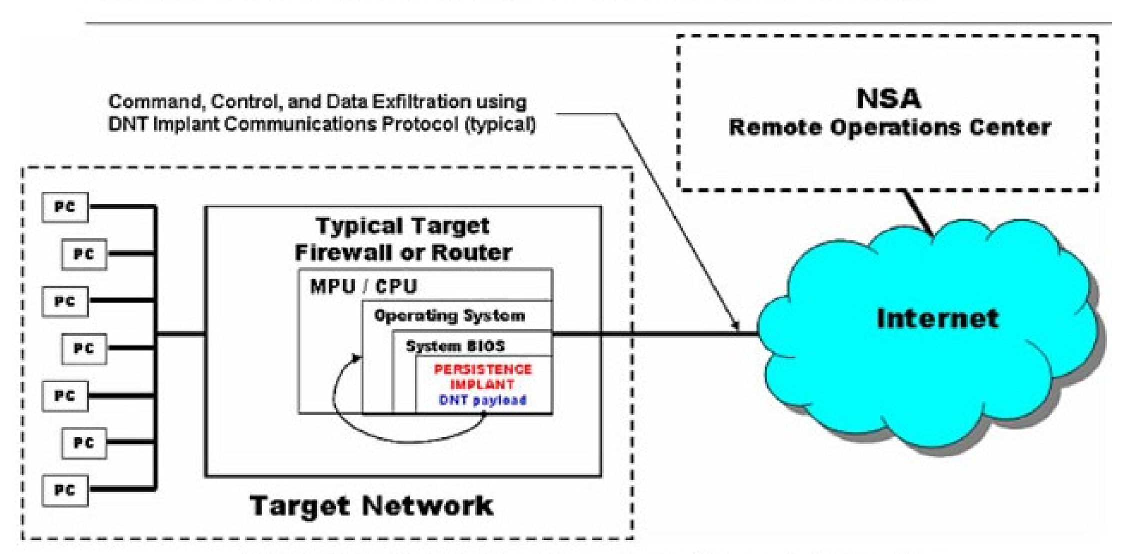


Imagen 16: Implante JETPLOW para equipos Cisco
Fuente: https://edwardsnowden.com

Una forma efectiva para implantar estas puertas traseras, es hacerlo antes de que los equipos sean entregados. Para esto se interceptan los paquetes, con equipamiento tecnológico, que son enviados a través del sistema de correo tradicional. Se abre el paquete interceptado para aplicar un implante y luego se lo devuelve al sistema de correo que lo entregará a su destino final. En la imagen 17 se puede ver el extracto de un documento donde a la izquierda se puede ver como se abre un equipo CISCO y a la derecha como se aplica el implante.[72]

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Imagen 17: Intercepción de ruteador Cisco para implantar puerta trasera
Fuente: https://edwardsnowden.com

Sería sencillo para la NSA interceptar los paquetes de equipos de redes que compran gobiernos extranjeros e implantar puertas traseras. De esta forma cuando los equipos estén instalados la NSA podrá recolectar información de redes donde se pensaba estarían seguras.

Se mostró algunas de las capacidades para ataques informáticos que tiene la NSA. Por otro lado, existen documentos que muestran que la criptografía en conjunto con software libre causan problemas para la vigilancia de esta agencia. Un documento filtrado muestra que la NSA no pudo descifrar un correo cifrados con PGP;[39][73] mientras que otro muestra que ocurrió lo mismo con una conversación de mensajería instantánea cifrada con OTR.[40][74]

La red de anonimato Tor representa un problema para la NSA. En la imagen 18 se puede ver una diapositiva de una presentación de 2012 que muestra que para la NSA Tor "apesta". En la misma presentación se menciona que la NSA nunca podrá espiar a todos los usuarios de esta red. [75]

39 Protocolo de cifrado para proteger correos electrónicos.
40 Protocolo de cifrado para proteger comunicaciones de mensajería instantánea.



Imagen 18: Presentación Tor Apesta
Fuente: https://edwardsnowden.com

Para solucionar los problemas relacionados con la criptografía, la NSA tiene el departamento de Servicio de Criptoanálisis y Explotación (CES por sus siglas en inglés). Según una investigación realizada por Der Spiegel, para el año 2013 CES tenía un presupuesto de $34.3 millones de dólares. [76]

Esta no es la única herramienta que tiene la NSA y la GCHQ para atacar el cifrado. The Guardian, [77] The New York Times[78] y Propublica[79] publicaron reportajes donde se analizan las estrategias de la agencia para vulnerar las comunicaciones seguras.

El alcance de este trabajo no contempló analizar estas investigaciones. Sin embargo, se las menciona por ser útiles como primera lecturas para quiénes quieran investigar sobre las capacidades de la agencia para atacar comunicaciones seguras.

3 Análisis de Información

En el capítulo anterior se analizó las formas en que la NSA almacena tráfico de comunicaciones. Ahora se verá como esta información es procesada para obtener contenidos relevantes de forma rápida. En una presentación se explica esta idea de manera precisa: “Se podría encontrar una aguja en un pajar de una forma repetitiva y eficiente”[41].[80]

Existen varios sistemas con los que la NSA analiza la información. XKEYSCORE es el que más información tiene disponible y parece ser la primera fuente de acceso a información. En 2009 tenía acceso a contenido de comunicaciones por tres días y metadatos de hasta treinta días. Información de blancos de vigilancia que la NSA considere más importantes se almacenan hasta por cinco años en el sistema PINWALE. La imagen 19 muestra una pirámide con algunos de los sistemas.[81]

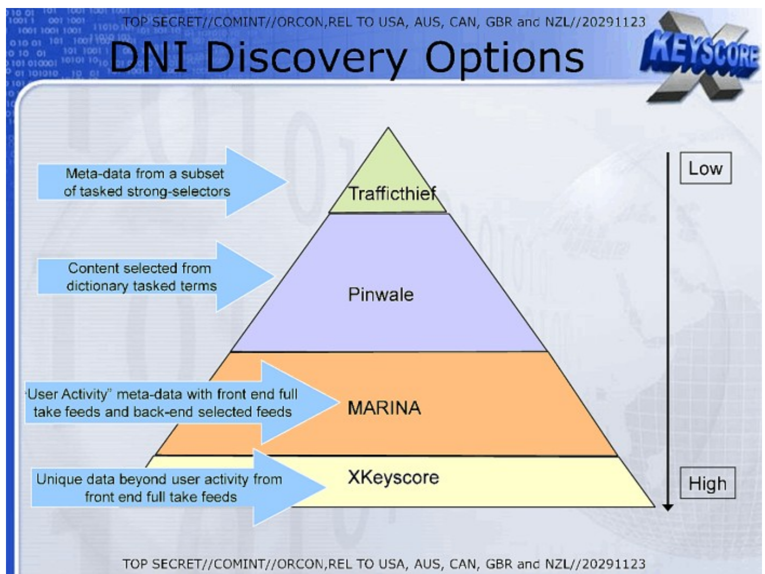


Imagen 19: Algunos sistemas de análisis de información
Fuente: https://edwardsnowden.com

41 Traducción propia: “Might find a needle in a haystack in a repetable and efficient way”

3.1 XKEYSCORE

"Yo, sentado en mi escritorio, tenía la facultad de intervenir al que fuera, desde un contador hasta un juez federal e incluso el presidente, siempre y cuando tuviera su correo electrónico personal." [82] Esa fue una de las afirmaciones más impactantes realizadas por Snowden en su primera entrevista realizada por The Guardian.[83]

El programa al que se refiere Snowden es XKEYSCORE. Este sistema permite hacer búsquedas sobre las comunicaciones recolectadas por la NSA a través de los sistemas vistos en el capítulo anterior. En general el contenido de las comunicaciones es almacenado durante tres días y los metadatos durante treinta.

La información es accedida desde varios de los sistemas vistos en el capítulo 2. La imagen 20 muestra una diapositiva de una presentación de 2008 donde se puede ver los sistemas sobre los que XKEYSCORE realiza consultas.[84]

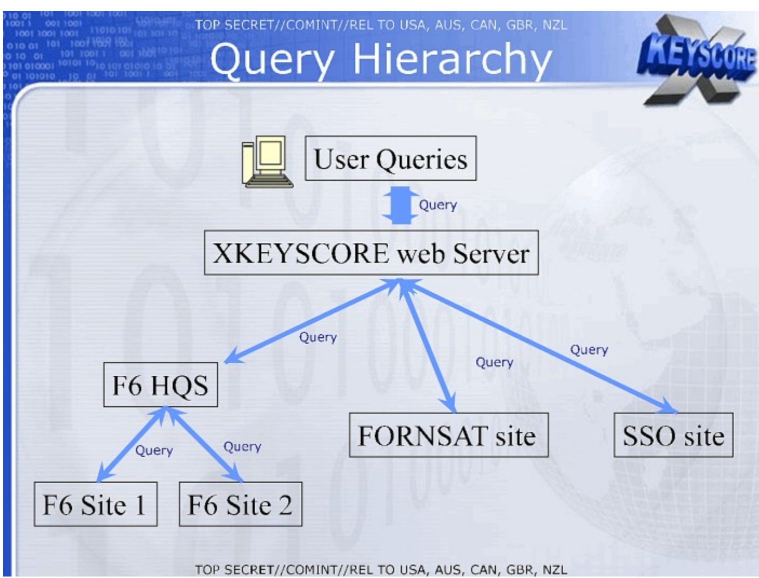


Imagen 20: Fuentes de información de XKEYSCORE

F6 hace referencia a los sitios de operaciones ubicados en embajadas alrededor del mundo (SCS).[85] FORNSAT se refiere a la información recolectada sobre las comunicaciones que viajan por Internet. SSO corresponde a la información recolectada en colaboración con

empresas. Los más probable es que refiera a los programas que participan dentro UPSTREAM. La información de PRISM se analiza en otros sistemas, como se verá más adelante.

Si bien la imagen 20 muestra algunas fuentes de información para XKEYSCORE, no son las únicas. Según otra presentación de 2008 se añaden como fuente de información TAO, FISA Y 3rd PARTY.[85]

Como se vio en el capítulo anterior 3rd PARTY hace referencia a la colaboración con otros países. Para 2012 la información recolectada por TEMPORA empezó a ser accesible a través de XKEYSCORE por lo que se convirtió en una de las fuentes de acceso más importante para este sistema. Con 1000 servidores era capaz de procesar 40 mil millones de registros. TEMPORA era “10 veces más grande que el segundo [sitio] XKEYSCORE”. [47]

En julio de 2015 The Intercept publicó una investigación sobre XKEYSCORE con 48 documentos de respaldo. Según la misma para 2008 XKEYSCORE estaba compuesto por 150 localidades alrededor del mundo y funcionaba con 700 servidores como se puede ver en la imagen 21.[86]

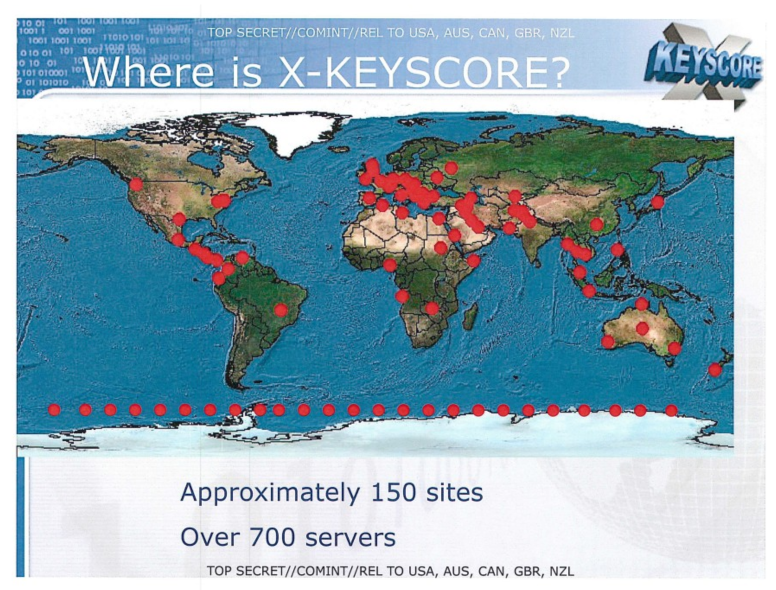


Imagen 21: Mapa de localidades de XKEYSCORE
Fuente: https://edwardsnowden.com

Con la información recolectada y almacenada en bases de datos MYSQL[42] distribuidas alrededor del mundo se puede realizar búsquedas de forma similar a las que se realizan en buscador de Internet. Existen formularios para buscar correos electrónicos, configuración de equipos informáticos, entre otros. En la imagen 22 se puede ver un ejemplo de formulario para capturar contraseñas de *webmails*.[87]

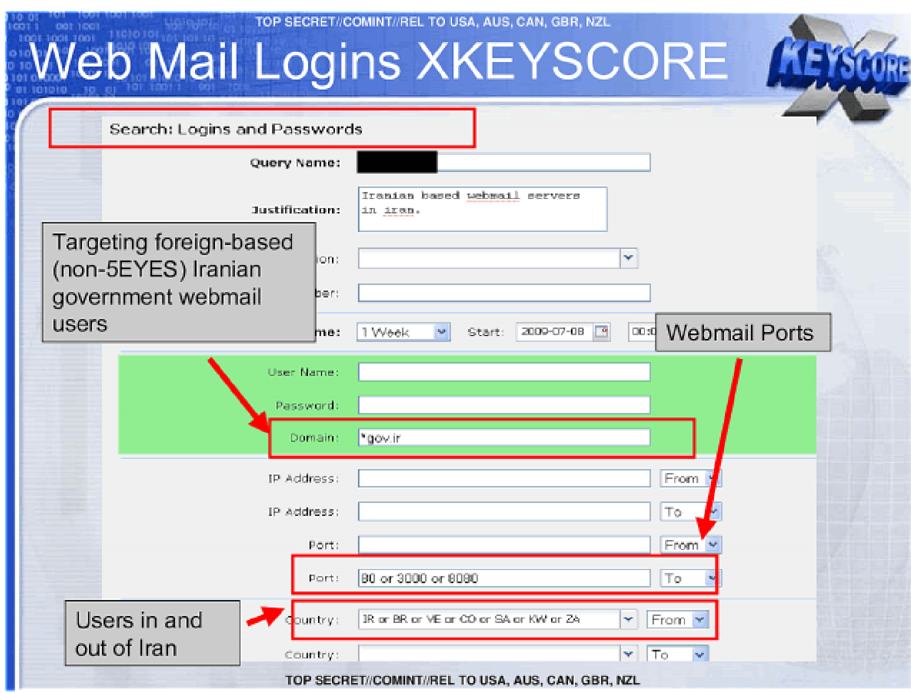


Imagen 22: Buscador de contraseñas de webmail
Fuente: https://edwardsnowden.com

La información que describe un correo electrónico tiene metadatos distintos a los de una página de Internet entregada por un servidor web a un navegador. De igual forma cada página es distintas a otras y tienen metadatos que las hace diferentes. Cosas tan simples como la dirección IP o el nombre de dominio son ejemplos de estos metadatos.

Para analizar el tráfico que viaja por Internet la NSA ha desarrollado un conjunto de reglas para el procesamiento de la información conocidos como identificadores de aplicaciones (AppIDs) y huellas digitales (Fingerprints). En los dos casos estos identificadores de tráfico añaden metadatos a la información recolectada para permitir realizar búsquedas muy específicas.[88]

42 Software libre que se utiliza como motor de bases de datos.

Los *AppIDs* permiten filtrar el tipo de aplicación según el tráfico almacenado. De esta forma se puede distinguir entre el tráfico que podría ser de navegación, de correo electrónico, entre otros. Además los identificadores permiten distinguir las aplicaciones de forma jerárquica. Se podría realizar la búsqueda del tráfico relacionado con el acceso al *webmail*, distinguirlo entre proveedores de *webmail* como Gmail o Yahoo; incluso dentro de cada proveedor se podría llegar a ser tan específico como el usuario y contraseña o un adjunto. La imagen 23 muestra una diapositiva que explica el funcionamiento jerárquico de los identificadores de aplicación. [88]

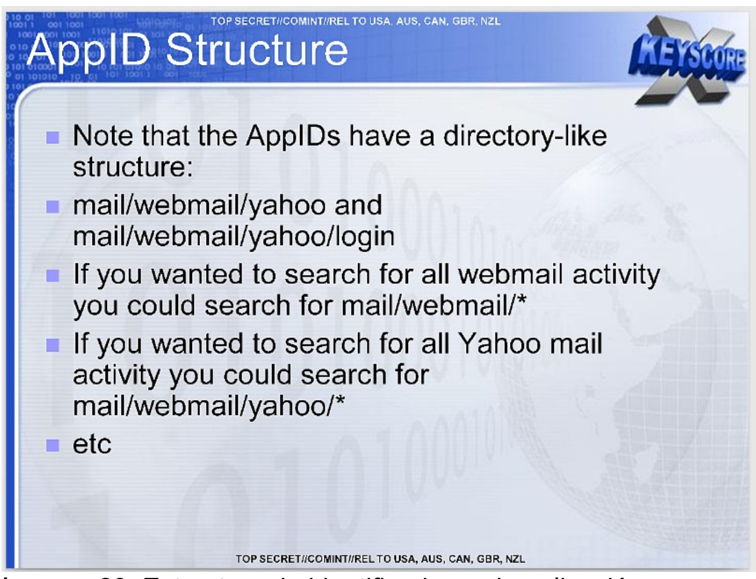


Imagen 23: Estructura de identificadores de aplicación
Fuente: https://edwardsnowden.com

La segunda forma en la que se identifica el tráfico es a través de F*ingerprints*. En este caso ya no se filtra el tráfico por una aplicación específica sino por una característica general. Estas podrían ser el idioma de la comunicación o si el tráfico está cifrado como se puede ver en la imagen 24.[88]

Imagen 24: Tráfico cifrado como ejemplo de fingerprint
https://edwardsnowden.com

3.1.2 Capacidades de búsqueda

Las búsquedas se las realiza sobre datos almacenados. Este tráfico se puede filtrar a través de los *AppIDs* y de los *Fingerprints*. Una analista podría leer el correo electrónico de sus blancos de vigilancia, robar usuarios y contraseñas, historial de navegación, analizar llamadas de voz/IP. Se podría pensar que XKEYSCORE es una herramienta similar a Wireshark[43] que funciona sobre el corazón de las comunicaciones de Internet.

La guía no oficial de XKEYSCORE escrita por Booz Allen Hamilton[44] explica algunos casos de uso para realizar búsquedas en este sistema. Se muestran formularios para realizar búsquedas dirección IP, dirección MAC, cuentas de correo, archivos adjuntos, usuarios y contraseñas, número de teléfono, actividad web, metadatos de documentos. Incluso se puede llegar a automatizar las búsquedas para facilitar la tarea del analista. [89]

Gran parte de estos ataques son vulnerables cuando se usa tráfico sin cifrar como el de los sitios web HTTP. Se entendería que gran parte de estos ataques se han visto afectados a través del uso de HTTPS. El

43 Herramienta de software libre utilizada para el análisis del tráfico de redes.
44 Empresa contratista de la NSA donde trabajaba Snowden al momento de filtrar los documentos.

buscador de Google lo hace desde octubre de 2011[90] y Gmail desde enero del 2010.[91] Por lo cuál se podría pensar que atacar a estos servicios sería difícil en la actualidad.

Salvo que la NSA tenga una copia de las llaves privadas de los certificados digitales de estas empresas, algo que no se puede ver en los documentos de Snowden. Otra posibilidad es que la NSA recolecte este tipo de información es a través de programas como MUSCULAR del que se habló en la sección 2.5.

Sea cual fuere el caso, en la actualidad gracias a las revelaciones de Snowden empresas como Google, Yahoo y Microsoft afirmaron tomar las medidas para proteger las comunicaciones entre sus centros de datos y protegerse así de ataques de la NSA.[66]

Debido a las revelaciones de Snowden, nació el proyecto Letsencrypt que permite añadir de forma fácil certificados válidos para sitios web. El objetivo de este proyecto es que el 100% de la web funcione en HTTPS. Para junio de 2017 Letsencrypt había emitido 100 millones de certificados.[92]

A pesar de las ventajas que puede brindar el cifrado, saber quién cifra puede generar información relevante para la NSA. En la imagen 25 se muestra una diapositiva de una presentación de 2008 que explica como se puede utilizar XKEYSCORE para extraer todo el tráfico PGP en un determinado país; en este caso Irán. Solo con metadatos y sin conocer el contenido de las comunicaciones se puede saber quién sé esta comunicando con quien de forma segura un país.[84]



Imagen 25: XKEYSCORE y cifrado
Fuente: https://edwardsnowden.com

Se vio algunos ejemplos de las capacidades de búsquedas que tiene XKEYSCORE. Se podría realizar todo un trabajo de investigación sobre esto proyecto. Sin embargo para el propósito del presente trabajo, queda claro que existe un *buffer* de tráfico de comunicaciones almacenada a nivel global sobre el cuál se puede realizar búsquedas.

3.2 Otros sistemas de análisis

Existen otros sistemas especializados donde se guarda información durante más tiempo para analizarla. Algunos de estos se los pueden ver en la diapositiva de PRISM que se muestra en la imagen 26. [29]

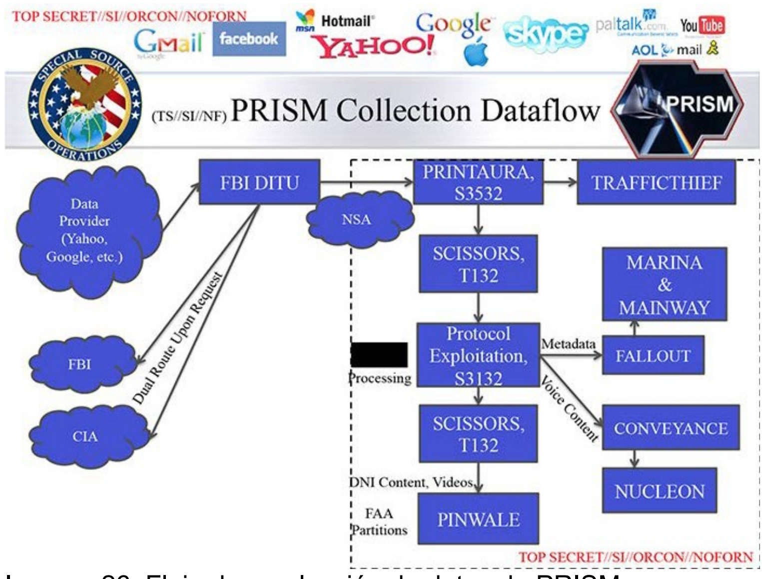


Imagen 26: Flujo de recolección de datos de PRISM
https://edwardsnowden.com

MAINWAY es un sistema que almacena y procesa metadatos recolectados por la NSA justificado legalmente en la sección 215 de la Ley Patriota. Este sistema procesa información tanto de señales de telefonía como comunicaciones de Internet.[93] Los metadatos procesados luego pasan a otro sistema conocido como MARINA donde se guarda la información por 365 días.[94]

NUCLEON se encarga del análisis de comunicaciones de voz. En este sistema es donde un analista busca las comunicaciones de llamadas voz/IP. La guía técnica para analizar comunicaciones de Skype en PRISM describe el caso de esta aplicación.[95]

En PINWALE se puede almacenar información hasta por cinco años. Se entiende que lo que hace un analista de la NSA es reenviar la información relevante desde XKEYSCORE para PINWALE donde se almacena tanto contenido como metadatos.[96]

Existen más sistemas que no se han analizado en este trabajo. Sin embargo, queda claro que la NSA dispone de XKEYSCORE como un buscador de propósito general y además dispone otros sistemas de propósito específico donde se almacena información por más tiempo.

4 Operaciones reveladas

Se podría pensar que los reportes realizados por la NSA son elaborados para la Casa Blanca, el ejercito o agencias como la CIA. La imagen 27 corresponde una documento confidencial donde se muestra que los clientes de la NSA incluyen a los departamentos de Agricultura, Tesoro, Comercio y Energía de Estados Unidos.[97]



Imagen 27: Clientes de la NSA
Fuente: https://edwardsnowden.com

A continuación se muestran algunos ejemplos de espionaje político realizado por la NSA que incluye a presidentes, sectores estratégicos y el espionaje a administradores de sistemas.

4.1 Espionaje político

Der Spiegel realizó un la investigación[98] sobre el espionaje a la canciller alemana Angela Merkel. En la misma se menciona una lista de 122 líderes políticos conocida como “Base de Conocimientos de Blancos de Vigilancia” (TKB por sus siglas en inglés). En la imagen 28 se puede ver una diapositiva de una presentación interna de 2009 en la que se muestran once de los miembros de esa lista.[99]

	Nymrod (machine-extracted) Citations				Last TKB Manual Update
	Name	Role	Code	Cites	
1	Abdullah Badawi	Malaysian Prime Minister	cos	> 100	10/15/2007
2	Abdullahi Yusuf	Somali President	cos	> 300	N/A
3	Abu Mazin	(Mahmud 'Abbas) PA President	cos	> 200	5/20/2009
4	Alan Garcia	Peruvian President	cos	> 100	N/A
5	Aleksandr Lukashenko	Belarusian President	cos	> 50	N/A
6	Alvaro Colom	Guatemalan President	cos	> 200	N/A
7	Alvaro Uribe	Colombian President	cos	> 700	N/A
8	Amadou Toumani Toure	Malian President	cos	> 50	N/A
9	Angela Merkel	German Chancellor	cos	> 300	N/A
10	Bashar al-Asad	Syrian President	cos	> 800	N/A
...	....	....	...		
122	Yuliya Tymoshenko	Ukrainian Prime Minister	cos	> 200	N/A

Imagen 28: Listado de líderes políticos espiados por la NSA
Fuente: https://edwardsnowden.com

Aparecen los diez primeros en el listado y el número 122, probablemente el último. Entre los miembros se puede ver, a los entonces presidentes de América Latina, Alan García de Perú, Álvaro Colom de Guatemala y Álvaro Uribe de Colombia.

Ellos no son los únicos presidentes latinoamericanos que han sido vigilados por la NSA. Según un reportaje de televisión de la cadena brasilera O Globo, Dilma Rousseff y Enrique Peña Nieto fueron espiados por la agencia.[100]

En el reportaje se muestra una presentación titulada “Filtrado Inteligente de tus datos: casos de estudio Brasil y México”.[45] La presentación trata sobre como a través de recolectar muchos datos se puede llegar a información relevante. En la misma se destaca a las operaciones realizadas a Rousseff y Peña Nieto como casos de éxito del filtrado inteligente de datos.[80]

En la imagen 29 se puede ver un gráfico que muestra como la NSA analiza las comunicaciones de un objetivo de vigilancia y sus principales contactos. Las comunicaciones directas entre el objetivo principal y las personas con las que se comunica se conoce como un salto. Cuando a este análisis se le añade la comunicación entre los contactos del blanco principal

45 Traducción propia: “Intelligently filtering your data: Brazil and Mexico case studies”

se conoce como 1.5 saltos. Cuando se muestra la comunicación entre los contactos se conoce como dos saltos.[80]

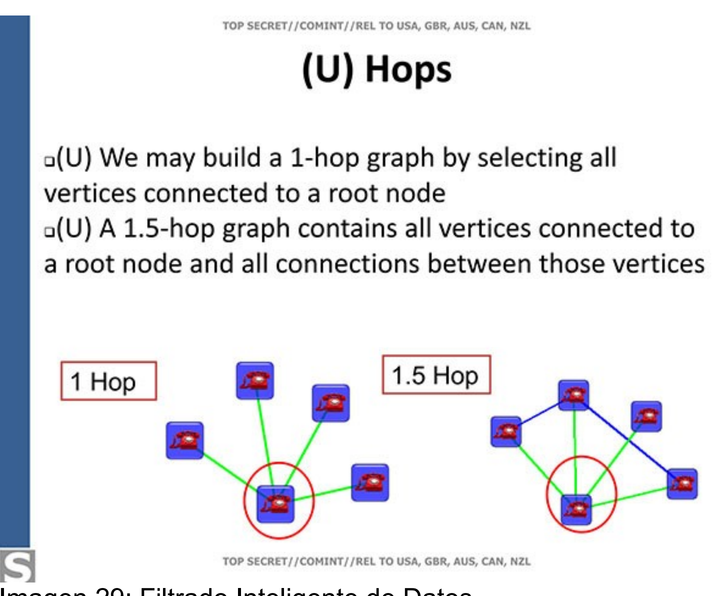


Imagen 29: Filtrado Inteligente de Datos
Fuente: https://edwarsnowden.com

Este es el tipo de análisis que se realizó a los dos presidentes. En la imagen 30 se puede ver el caso de Rousseff, ella y sus asesores cercanos fueron espiados cuando era presidenta.[80] Según el reportaje de la cadena O Globo, el espionaje a Dilma se lo realizó a través de su teléfono celular, correo electrónico y dirección IP.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Imagen 30: Diapositiva espionaje a Dilma Rousseff
Fuente: https://edwardsnowden.com

El caso de espionaje a Peña Nieto, sucedió cuando él era el candidato presidencial con mayores posibilidades en las elecciones de 2012.

La vigilancia se la hizo a él y nueve de sus asesores más cercanos durante dos semanas como se puede ver en la imagen 31.[80]



Imagen 31: Diapositiva espionaje a Enrique Peña Nieto
Fuente: https://edwardsnowden.com

Dice el reporte que se interceptaron y analizaron 85 489 mensajes SMS para extraer los más importantes. En la presentación se pueden ver capturas de pantalla de mensajes donde se mencionan posibles futuros miembros de gobierno. Según O Globo esas personas fueron luego nombradas miembros del gobierno.

Este no es el único caso en el que el un líder mexicano ha sido espiado por la NSA. Der Spiegel hizo una investigación sobre el espionaje que Estados Unidos realizó a su vecino del sur.[101] En la misma se publicó el extracto de un documento de noviembre de 2010 donde se dice que el equipo de TAO logró tener acceso a los correos del dominio de la presidencia de México. Gracias a lo cuál se pudo acceder al correo electrónico del presidente. Dice el documento "El dominio [de correo electrónico] atacado es también utilizado por el gabinete mexicano y contenía comunicaciones diplomáticas, económicas y de liderazgo que continúan proporcionando una visión del sistema político mexicano y de la estabilidad interna."[46][102]

46 Traducción propia del inglés "The targeted domain, also used by the Mexican cabinet, contained diplomatic, economic and leadership communications which continue to provide insight into Mexico's political system and internal stability."

Argentina tampoco se salva de los programas de la Alianza de los Cinco Ojos. Para la GCHQ el país del sur es su principal interés en América Latina. Para mejorar la imagen de Reino Unido en relación con las Islas Malvinas, la GCHQ preparó la operación QUITO. En abril de 2015, The Intercept[103] y Todo Noticias[104] de Argentina reportaron en conjunto sobre esta operación.

La operación QUITO se llevó acabo por el Grupo de Tareas Contra Amenazas (JTRIG por sus siglas en inglés). En la imagen 32 se puede ver que para 2009 la operación estaba lista para llevarse a cabo por un periodo largo, a gran escala y con efectos pioneros.[105]

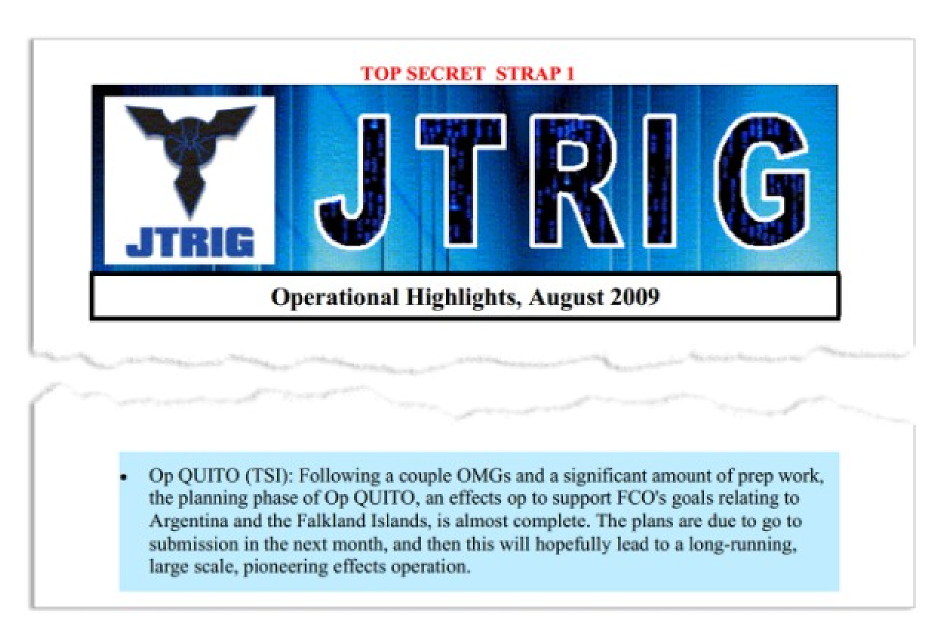


Imagen 32: JTRIG y la operación QUITO
Fuente: https://edwardsnowden.com

JTRIG es una unidad de trabajo dentro de la GCHQ que se encarga de desinformar en Internet y desacreditar a personas. Para esto realiza campañas en redes sociales con el fin de dañar la imagen de sus adversarios.[106]

Las operaciones de la GCHQ en Argentina no se limitaron a JTRIG y la operación QUITO. En la imagen 33 se puede ver otro documento que muestra el interés de recolectar la comunicación de líderes y militares.

Target Areas/Tasking (362s):

Argentina

TSI initiated and supported OH tasking against Argentina in efforts to collect high priority military and Leadership comms. Work was coordinated across the OH enterprise to obtain results when opportunity arose using US 903G and US 940C, MHS Ops were a main driver for this collection. Results included a number of TETRA collects and at least seven Argentinian PCM (digital) microwave emitters which were processed and geolocated. Although TSI haven't got desired results on their comms of interest as yet, this was a positive and encouraging team effort against this target in readiness for when next opportunity arises. Efforts between TSI and MHS continue.

Imagen 33: Espionaje a líderes y militares argentinos
Fuente: https://edwardsnowden.com

A pesar de que estas revelaciones fueron noticia en la televisión Argentina y que los documentos de Snowden lo han sido a nivel mundial. Parece ser que las autoridades no entienden el riesgo de la vigilancia masiva, en especial en la educación. El gobierno de la Ciudad de Buenos Aires distribuye computadoras instaladas el sistema operativo Windows 10 de Microsoft. Esto implica poner en riesgo la privacidad de los estudiantes como explica Esteban Magnani, periodista Argentino, en su blog:

> De nuestras escuelas saldrán funcionarios, empresarios, legisladores (por qué no) algún presidente/a. Microsoft podrá conocer detalles sobre sus intereses, su desarrollo, sus contactos y hasta conocer su voz o su ubicación a lo largo de su vida. Que el Estado argentino se plantee la posibilidad de brindar datos de sus ciudadanos va en contra de las leyes de privacidad de datos (y no es la primera vez).[107]

Este es solo un ejemplo. El uso de herramientas de empresas de PRISM es ampliamente utilizado en la educación alrededor del mundo.

4.2 Espionaje a sectores estratégicos

La empresa de petróleos de Venezuela (PDVSA) es un objetivo de interés para la NSA. Según un boletín interno de 2011, PDVSA resulta interesante ya que representa el 80% de las exportaciones del país y más de la mitad de los ingresos económicos del gobierno. [108]

Según el boletín, se solicitó a un analista realizar una investigación a los directivos de PDVSA. Para esto el analista buscó en sistemas y bases de datos como CADENCE, PINWALE y UTT. Luego del trabajo realizado se

pudo extraer información de los entonces presidente de PDVSA Rafael Ramírez y vicepresidente Luis Felipe Vierma Pérez.

El analista destaca que, sin saberlo, la NSA ya había recolectado información de PDVSA. Según el reportaje de The Intercept, donde se publicó este documento, esto es una muestra de como la NSA tiene más información de la que puede manejar. [109]

Al igual que Venezuela, Brasil es otro país con recursos naturales que resultan interesantes para la Alianza de los Cinco Ojos. El Centro Seguridad de las Comunicaciones (CSEC por sus siglas en Inglés), es el equivalente a la NSA en Canadá. Según un reportaje de la cadena O Globo la NSA y CSEC trabajaron en conjunto para espiar las comunicaciones de del Ministerio de Minas de Brasil.[110]

El reportaje destaca que tres de las cuatro empresas mineras más grandes del mundo son canadienses. Motivo por el cuál el espionaje económico sobre los recursos mineros de Brasil resulta estratégico para Canadá.

4.3 Ataques a administradores de sistemas

El trabajo de un administrador de sistemas consiste en gestionar los sistemas que utiliza una organización. Es el responsable de la operación de herramientas como el servicio de correo electrónico, servidor de archivos, servidor de páginas web, etcétera. Si se logra vulnerar un dispositivo de un administrador de sistemas entonces sería fácil acceder a la información que se almacena en los sistemas que gestiona.

En un foro interno de la NSA, un especialista describe esta característica de la siguiente forma: “¿A quién mejor vigilar que a la persona que ya tiene las ‘llaves del reino’?”[47][111, p. 3]

Para comprometer los equipos de un administrador de sistemas recomienda identificar las cuentas personales de correo electrónico y redes

47 Traducción propia del inglés: “… who better to target than the person that already has the ‘keys to the kingdom?”

sociales del blanco de vigilancia. Esto se debe a que la NSA dispone de herramientas para implantar programas maliciosos a alguien que quiere acceder a un servicio de *webmail* o una red social como Facebook.

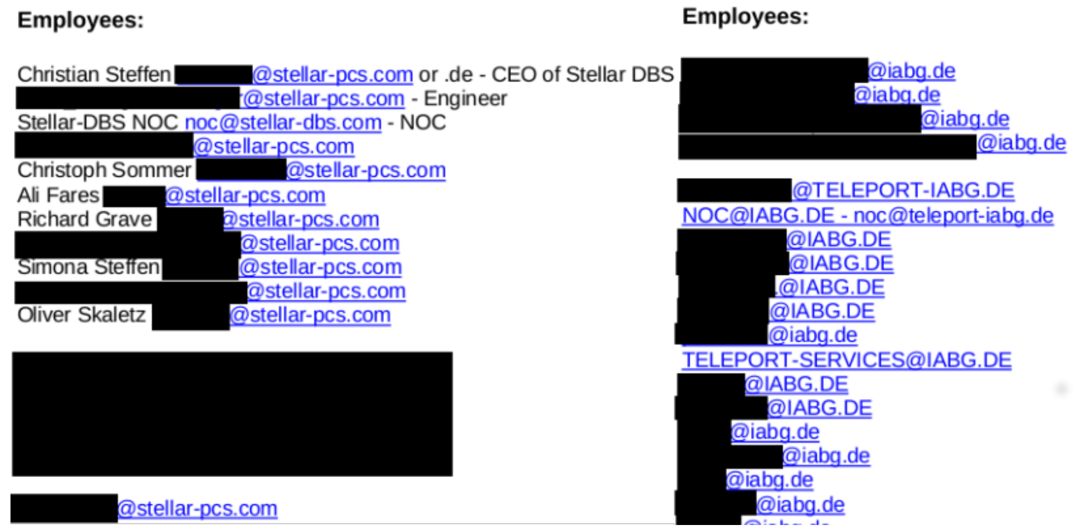
Una vez que se tiene control sobre la computadora del administrador el analista de la NSA tendrá acceso a información como la documentación de la red, cuentas de acceso, incluso podría instalar un *keylogger*[48] para capturar las contraseñas mientras las escribe.[112]

Los administradores sistemas de proveedores de Internet resultan interesantes ya que tienen acceso a redes donde fluye mucha información. Se podría capturar el tráfico de Internet de países enteros. El autor de estas publicaciones dice "imagina correr Wireshark dentro un ruteador de un ISP"[49][111, p. 6]

En la sección 2.5 del presente trabajo se explicó como la NSA atacó a varios proveedores de Internet para poder recolectar información de sus clientes. Uno de estos era la empresa alemana Stellar que provee servicio de Internet satelital en varios continentes.

En el reportaje que realizó Der Spiegel sobre el ataque a Stellar y otros proveedores de Internet hay un video con una entrevista. Uno de los entrevistados fue Ali Fares, miembro del equipo ingenieros de esta Stellar. En la entrevista se le muestra a Fares documentos de la NSA con información de la red de la empresa y a quiénes espiaron.[68] En la imagen 33 se puede ver un listado de los empleados espiados dentro de la empresa; entre los nombres consta el de Ali Fares.[69]

48 Herramienta utilizada para capturar las teclas pulsadas por un teclado. Comúnmente se utiliza para capturar contraseñas.
49 Traducción propia del inglés: "...imagine running Wireshark on an ISP's infrastructure router "



TOP SECRET STRAP1

Employees:

Christian Steffen [redacted]@stellar-pcs.com or .de - CEO of Stellar DBS
[redacted]@stellar-pcs.com - Engineer
Stellar-DBS NOC noc@stellar-dbs.com - NOC
[redacted]@stellar-pcs.com
Christoph Sommer [redacted]@stellar-pcs.com
Ali Fares [redacted]@stellar-pcs.com
Richard Grave [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Simona Steffen [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Oliver Skaletz [redacted]@stellar-pcs.com

[redacted]

[redacted]@stellar-pcs.com

TOP SECRET

Employees:

[redacted]@iabg.de
[redacted]@iabg.de
[redacted]@iabg.de
[redacted]@iabg.de

[redacted]@TELEPORT-IABG.DE
NOC@IABG.DE - noc@teleport-iabg.de
[redacted]@IABG.DE
[redacted]@IABG.DE
[redacted]@IABG.DE
[redacted]@IABG.DE
[redacted]@iabg.de
TELEPORT-SERVICES@IABG.DE
[redacted]@IABG.DE
[redacted]@IABG.DE
[redacted]@iabg.de
[redacted]@iabg.de
[redacted]@iabg.de
[redacted]@iabg.de

Imagen 34: Empleados de proveedores de Internet vigilados por NSA y GCHQ
Fuente: https://edwardsnowden.com

Los administradores de sistemas informáticos tienen mucha responsabilidad. La seguridad sobre las comunicaciones que deben proteger no se limita a las de su trabajo. Sus correos electrónicos y redes sociales son objetivos de vigilancia para la NSA. Es por esto que se debe sensibilizar sobre seguridad informática en sus comunicaciones privadas.

Conclusiones

Las filtraciones de Snowden permiten entender el funcionamiento de la NSA. La información analizada en esta investigación explica la forma en la que, esta agencia, recolecta y analiza información. Estas capacidades son utilizadas luego para operaciones de espionaje que buscan beneficios políticos y económicos para los miembros de la Alianza de los Cinco Ojos.

Las estrategias de espionaje de la NSA no son nuevas. Motivada por la guerra fría desarrolló tecnologías para la inteligencia de señales. La embajada de Moscú se utilizó para espiar al gobierno Ruso en los años 1960s. El programa ECHELON, revelado en 1988, se utilizó para espiar y analizar comunicaciones satelitales a nivel mundial. La red de internacional de telégrafo que atravesaba los Estados Unidos se utilizó para interceptar comunicaciones. Incluso la colaboración de empresas tecnológicas para el espionaje se lo hacía hace mucho, como se pudo ver en el caso de RCA y el sistema de telefonía de Cuba en 1959.

Las prácticas no cambiaron pero la tecnología sí. El uso de las tecnologías de la información y comunicación (TICs) es cada vez mayor. No se puede negar que esto trae beneficios para la sociedad. Nunca antes fue tan fácil y económico acceder a tanta información y conocimiento. Además, ahora es posible comunicarse con una persona en cualquier parte del mundo de una forma inmediata y económica.

De la misma manera, nunca antes fue tan barato vigilar la actividad de las personas y sus comunicaciones. La vida digital deja huella y las empresas, pertenecientes a PRISM y otras, utilizan esta huella para ofertar productos a través de publicidad direccionada. Agencias como el FBI, la CIA o la NSA pueden solicitar la información almacenada en los servidores de empresas de PRISM para espiar a cualquiera persona que no sea ciudadano de Estados Unidos sin ningún control.

A pesar de que todo esto ya se sabía, los servicios y productos de las empresas de PRISM son ampliamente utilizados. Los medios de

comunicación cubren el lanzamiento de los últimos teléfonos de Apple con características como reconocimiento facial para desbloquearlo. Sin embargo, no se pone en duda, ante la opinión pública, el hecho de que esta empresa podría estar proveyendo el reconocimiento facial a agencias de inteligencia. Hacen lo contrario y en lugar de periodismo crítico realizan publicidad.

Las compañías de telefonía móvil ofertan promociones de WhatsApp ilimitado sin consumo en planes de datos. Esto sucede a pesar de que WhatsApp fue comprada por Facebook en el año 2014 y esta última es miembro de PRISM. Los usuarios de estos servicios deben estar informados sobre quiénes son sus proveedores, lo que podrían hacer con sus datos y las implicaciones con su privacidad.

Los centros de educación deben ser lugares donde las nuevas generaciones se eduquen sobre los riesgos de la pérdida de la privacidad en un mundo cada vez más digitalizado. También se debe usar la educación para aprender a proteger las comunicaciones. A pesar de esto, se utilizan cada vez más los servicios en la nube provistos por empresas como Microsoft o Google. ¿Son consientes las autoridades de los centros de educación sobre las implicaciones a la privacidad de estos servicios?

Los gobiernos están obligados a defender los derechos humanos de sus ciudadanos. La privacidad es uno de ellos y se debe hacer lo posible para protegerla. Sobretodo cuando a privacidad de la vida digital de sus ciudadanos es vulnerada por empresas y gobiernos extranjeros.

En lugar de hacer esto, muchos gobiernos llegan a colaborar con estas empresas y poner en riesgos a sus ciudadanos. Este es el caso de Argentina donde se busca llegar a acuerdos con empresas como Facebook o Amazon. En el caso del último se quiere cambiar la ley de protección de datos personales para que se puedan alojar los datos en servidores de Amazon fuera del país.

La centralización de las comunicaciones en servicios provistos por empresas norteamericanas, es quizás, la mayor fortaleza de la NSA. La información accedida a través de PRISM es la principal fuente de la agencia

para generar informes. Incluso cuando no se usa estos servicios, es muy probable que la las comunicaciones atraviesen infraestructura controlada por la NSA. En ese caso también es interceptada y almacenada para posterior su análisis.

Cuando la información no atraviesa por un medio tecnológico controlado por la NSA, la agencia tiene recursos destinados para salir a buscarla. Esto lo hace espiando comunicaciones celulares a través de decenas de misiones diplomáticas en el mundo o las comunicaciones satelitales desde estaciones terrestres. Cuando esto no es suficiente, existe TAO que se encarga de realizar ataques informáticos para intentar recolectar todo.

Sobre todo este mar de información recolectada, la NSA tiene la capacidad de realizar búsquedas muy precisas. De manera similar al funcionamiento de buscadores como el de Google o Duckduckgo, la agencia tiene herramientas que permiten realizar búsquedas sobre las comunicaciones interceptadas. Es decir las comunicaciones de miles de millones de personas en el mundo.

XKEYSCORE, en 2009, tenía la capacidad de realizar búsquedas sobre tres días de contenido y treinta días de metadatos de comunicaciones interceptadas. Para objetivos de vigilancia importantes existen otros sistemas como PINWALE donde la información se almacenaba hasta por cinco años. Es probable que en la actualidad estos tiempos sean mayores.

La criptografía complica el trabajo de herramientas como XKEYSCORE. Parte del poder que tiene esta herramienta se debe a que la mayoría de actividad que se realiza en Internet se lo hace a través del protocolo inseguro HTTP. Los grandes sitios de Internet, cada vez más, utilizan en sus portales el protocolo seguro HTTPS. Los medianos y pequeños ahora pueden proteger sus sitios a través de Letsencrypt. Un paso importante para dificultar las operaciones de análisis de la NSA.

La NSA justifica el uso de estas herramientas para proteger a los Estados Unidos de la amenaza del terrorismo. Espionaje a presidentes y a

sectores estratégicos de países como Brasil y Venezuela. Manipulación de la forma de pensar de poblaciones enteras como la operación QUITO para mejorar la imagen de Gran Bretaña con respecto a las Malvinas en América Latina. Son algunos de los ejemplos que se mostraron en este trabajo pero no son los únicos.

La NSA busca capturar la información que fluye a través de las redes informáticas. Un ejemplo de aquello es el caso del proveedor de Internet alemán Stellar que provee servicios de Internet satelital a varios continentes. Sus empleados fueron espiados para tomar control sobre su red. En este y otros casos los administradores de sistemas se convierten en blancos estratégicos de vigilancia.

En América Latina las empresas Telefónica y Claro tiene presencia en la mayoría de países. La cantidad de información que fluye por las redes de estos proveedores debe ser apetecido por la NSA y agencias de otros países. ¿Qué tan protegidas están estas redes de la NSA y otras agencias? ¿Se preocupan por proteger la privacidad de sus clientes? Por las promociones que ofertan servicios de empresas PRISM se debe, al menos, desconfiar.

Edward Snowden arriesgó su vida para alertar a la sociedad sobre los riesgos de la vigilancia de la NSA. Si bien se ha generado debate al respecto y cada vez más gente conoce los riesgos sobre la pérdida de la privacidad. Los servicios centralizados en la nube siguen siendo los principales medios de comunicación de las personas que usan Internet. Ramonet sostiene que para resistir la vigilancia:

> La solución está en buscar una multitud de microresistencias, que pasan por la educación popular, la formación en herramientas informáticas de cifrado, la búsqueda de soluciones alternativas para volver caducas las actuales normas dominadas por las GAFAM[50].[15, p. 98]

50 Cuando Ramonet hace referencia a GAFAM se refiere a las empresas: Google, Amazon, Facebook, Apple y Microsoft

El cifrado extremo a extremo[51]utilizado en protocolos como OTR y PGP ha demostrado causar problemas a la NSA. Para proteger la privacidad de las comunicaciones en Internet se debe cifrar la mayor cantidad de comunicaciones con este tipo de tecnología.

El uso herramientas como Tor permiten el anonimato en Internet cuando se lo utiliza de manera correcta. Además si se trabaja con pseudónimos se puede llegar a esconder los metadatos. Es decir quién se comunica con quién.

A diferencia del software privativo, el software libre puede ser auditado porque su código fuente es público. Sin embargo, no todo el software libre es auditado. Se necesita organizar a la sociedad civil, academia y Estado para auditar estos sistemas.

Otra característica de los sistemas libres es que no tienen una barrera económica para su acceso. Por lo que su uso se puede masificar sin discriminar entre ricos y pobres. La barrera que existe con el software libre es que es poco conocido en la sociedad y su adopción requiere cambios de hábitos. Una vez más sociedad civil, academia y Estado deben unir fuerzas para acercar estas herramientas a la población.

Internet se debe descentralizar para volver a ser la red de redes que fue en su inicio. De esta manera la información no estará disponible para la NSA, como sucede con los servicios de empresas PRISM, sino que deberá salir a buscarla. Las redes P2P tienen la ventaja adicional que no requieren servidores centralizados por donde se podría espiar las comunicaciones.

Más allá de la tecnología utilizada, es importante crear conciencia en la ciudadanía sobre la importancia de la seguridad informática para conservar la privacidad en el siglo veintiuno. Solo una sociedad educada sabrá proteger sus derechos y buscar los medios para hacerlo.

51 Cifrado extremo a extremo quiere decir que la comunicación se cifra entre los extremos de la comunicación. Es decir, quién administre el servidor no podrá leer las comunicaciones. En inglés se utiliza se suele utilizar “end-to-end encryption”.

Bibliografía

Específica

[1] M. Aid, *The Secret Sentry: The Untold History of the National Security Agency*, First Edition edition. New York: Bloomsbury Press, 2009.

[2] J. Risen y E. Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts”, *The New York Times*, 16-dic-2005. [En línea]. Disponible en: https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html. [Consultado: 11-jul-2017].

[3] “Verizon FISA Court order”. [En línea]. Disponible en: https://edwardsnowden.com/2013/06/06/verizon-fisa-court-order/. [Consultado: 28-sep-2017].

[4] G. Greenwald, “NSA collecting phone records of millions of Verizon customers daily”, *The Guardian*, 06-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. [Consultado: 17-abr-2017].

[5] Gellman, Barton y Poitras, Laura, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program - The Washington Post”, 06-jul-2013. [En línea]. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. [Consultado: 16-oct-2016].

[6] Greenwald, Glenn, *Snowden. Sin un Lugar Donde Esconderse*, 1a ed. Colombia: Ediciones B, 2014.

[7] L. Poitras, *Citizenfour*. Radius-TWC, 2014.

[8] Greenwald, Glenn, “On leaving the Guardian”, *The Guardian*, 31-oct-2013. [En línea]. Disponible en: https://www.theguardian.com/commentisfree/2013/oct/31/glenn-greenwald-leaving-guardian. [Consultado: 17-ene-2017].

[9] “NSA General Keith Alexander: ‘Snowden betrayed us’”, 23-jun-2013. [En línea]. Disponible en: http://www.bbc.com/news/world-us-canada-23022932. [Consultado: 01-mar-2017].

[10] Obama, Barak, “Statement by the President”, *whitehouse.gov*, 07-jun-2013. [En línea]. Disponible en: https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president. [Consultado: 17-abr-2017].

[11] E. Saiz, “Rousseff condena las prácticas de espionaje ante las Naciones Unidas | Internacional | EL PAÍS”, 24-sep-2013.

[12] Donohue, Laura K., “NSA surveillance may be legal — but it’s unconstitutional”, *Washington Post*, 21-jun-2013. [En línea]. Disponible en: https://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html. [Consultado: 21-jul-2017].

[13] ACLU, “Surveillance Under the USA/PATRIOT Act”, *American Civil Liberties Union*. [En línea]. Disponible en: https://www.aclu.org/other/surveillance-under-usapatriot-act. [Consultado: 23-jul-2017].

[14] EFF, “702 One Pager Adv | Electronic Frontier Foundation”. [En línea]. Disponible en: https://www.eff.org/document/702-one-pager-adv. [Consultado: 24-jul-2017].

[15] Ramonet, Ignacio, *El Imperio de la Vigilancia*, Primera edición. Buenos Aires: Capital Intelectual, 2016.

[16] D. Campbell, “Bajo la vigilancia de los Cinco Ojos”, *EL PAÍS*, 07-jul-2013. [En línea]. Disponible en:

https://internacional.elpais.com/internacional/2013/07/05/actualidad/1373038892_139217.html. [Consultado: 16-jul-2017].
[17] "La Declaración Universal de Derechos Humanos", 06-oct-2015. [En línea]. Disponible en: https://www.un.org/es/universal-declaration-human-rights/. [Consultado: 24-jul-2017].
[18] "Constitución del Ecuador". [En línea]. Disponible en: http://www.asambleanacional.gob.ec/documentos/constitucion_de_bolsillo.pdf.
[19] R. Bonifaz, "Entrevista a Rodrigo Iglesias | Rafael Bonifaz". [En línea]. Disponible en: https://rafael.bonifaz.ec/blog/2017/09/entrevista-a-rodrigo-iglesias/. [Consultado: 26-sep-2017].
[20] "Diputados piden explicaciones por la implementación de Facebook at Work en el Estado nacional", 18-mar-2016. [En línea]. Disponible en: http://www.lanacion.com.ar/1880973-dudas-por-la-implementacion-de-facebook-at-work-en-el-estado. [Consultado: 14-sep-2017].
[21] F. Spinetta, "Todos los datos al servicio de las empresas | El Gobierno firmó un memorándum con Amazon", *PAGINA12*, 13-jul-2017. [En línea]. Disponible en: https://www.pagina12.com.ar/49913-todos-los-datos-al-servicio-de-las-empresas. [Consultado: 14-sep-2017].
[22] "Edward Snowden Interview: The NSA and Its Willing Helpers - SPIEGEL ONLINE - International", *SPIEGEL ONLINE*, 08-jul-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html. [Consultado: 03-mar-2017].
[23] "Mass Surveillance | Privacy International". [En línea]. Disponible en: https://www.privacyinternational.org/node/52. [Consultado: 01-feb-2017].
[24] G. Greenwald y E. MacAskill, "Boundless Informant: the NSA's secret tool to track global surveillance data", *The Guardian*, 11-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. [Consultado: 19-jun-2017].
[25] "Boundless Informant heat maps". [En línea]. Disponible en: https://edwardsnowden.com/2014/05/14/boundless-informant-heat-maps/. [Consultado: 23-sep-2017].
[26] "Worldwide SIGINT/Defense Cryptologic Platform". [En línea]. Disponible en: https://edwardsnowden.com/2013/11/23/worldwide-sigintdefense-cryptologic-platform/.
[27] "NSA's global interception network", *Electrospaces.net*, 03-dic-2013. [En línea]. Disponible en: https://electrospaces.blogspot.com.ar/2013/12/nsas-global-interception-network.html. [Consultado: 19-jun-2017].
[28] "NSA Strategic Partnerships | Courage Snowden". [En línea]. Disponible en: https://edwardsnowden.com/2014/05/15/nsa-strategic-partnerships/. [Consultado: 29-jun-2017].
[29] "PRISM/US-984XN Overview". [En línea]. Disponible en: https://edwardsnowden.com/2013/06/07/prism-overview-slides/.
[30] "Special Source Operations overview". [En línea]. Disponible en: https://edwardsnowden.com/2013/11/05/special-source-operations-overview/. [Consultado: 30-jul-2017].
[31] J. Angwin, C. Savage, J. Larson, H. Moltke, L. Poitras, y J. Risen, "AT&T Helped U.S. Spy on Internet on a Vast Scale", *The New York Times*, 15-ago-2015. [En línea]. Disponible en: https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html. [Consultado: 22-jun-2017].
[32] "SSO Corporate Portfolio Overview". [En línea]. Disponible en: https://edwardsnowden.com/2015/08/18/sso-corporate-portfolio-overview/. [Consultado: 30-jun-2017].
[33] S. Ackerman, "Snowden disclosures helped reduce use of Patriot Act provision to acquire email records", *The Guardian*, 29-sep-2016. [En línea]. Disponible en:

https://www.theguardian.com/us-news/2016/sep/29/edward-snowden-disclosures-patriot-act-fisa-court. [Consultado: 14-jul-2017].
[34] Humphries, Matthew, "Dropbox Bug Restores Files Deleted 7 Years Ago | News & Opinion | PCMag.com", 24-ene-2017. [En línea]. Disponible en: http://www.pcmag.com/news/351256/dropbox-bug-restores-deleted-files-7-years-later. [Consultado: 03-mar-2017].
[35] "New insights into the PRISM program", 21-ene-2016. [En línea]. Disponible en: http://electrospaces.blogspot.com/2013/07/new-insights-into-prism-program.html. [Consultado: 04-mar-2017].
[36] G. Greenwald y E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 07-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. [Consultado: 16-oct-2016].
[37] "NSA slides explain the PRISM data-collection program", *The Washington Post*, 07-oct-2013. [En línea]. Disponible en: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. [Consultado: 30-sep-2016].
[38] Zetter,Kim, "Google's Real Secret Spy Program? Secure FTP", *WIRED*, 12-jun-2013. [En línea]. Disponible en: https://www.wired.com/2013/06/google-uses-secure-ftp-to-feds/. [Consultado: 06-mar-2017].
[39] Miller, Claire Clain, "Tech Companies Concede to Surveillance Program - The New York Times", 07-jun-2013. [En línea]. Disponible en: http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html. [Consultado: 02-ene-2017].
[40] G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, y D. Rushe, "Microsoft handed the NSA access to encrypted messages", *The Guardian*, 12-jul-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data. [Consultado: 09-mar-2017].
[41] Agwin, Julia, J. Larson, C. Savage, J. Risen, H. Moltke, y L. Poitras, "NSA Spying Relies on AT&T's 'Extreme Willingness to Help'", *ProPublica*, 15-ago-2015. [En línea]. Disponible en: https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help. [Consultado: 31-jul-2017].
[42] Gallagher, Ryan y H. Moltke, "The NSA's Spy Hub in New York, Hidden in Plain Sight", *The Intercept*. [En línea]. Disponible en: https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/. [Consultado: 31-jul-2017].
[43] P. Farrell, "History of 5-Eyes – explainer", *The Guardian*, 02-dic-2013. [En línea]. Disponible en: http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer. [Consultado: 19-jul-2017].
[44] E. MacAskill, J. Borger, N. Hopkins, N. Davies, y J. Ball, "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. [Consultado: 08-feb-2017].
[45] "Tempora". [En línea]. Disponible en: https://edwardsnowden.com/2014/07/21/tempora/.
[46] J. Ball, L. Harding, y J. Garside, "BT and Vodafone among telecoms companies passing details to GCHQ", *The Guardian*, 02-ago-2013. [En línea]. Disponible en: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq. [Consultado: 28-jun-2017].
[47] "TEMPORA — "The World's Largest XKEYSCORE" — Is Now Available to Qualified NSA Users". [En línea]. Disponible en: https://edwardsnowden.com/2014/07/23/tempora-the-worlds-largest-xkeyscore-is-now-available-to-qualified-nsa-users/.
[48] E. MacAskill, J. Borger, N. Hopkins, N. Davies, y J. Ball, "Mastering the internet: how GCHQ set out to spy on the world wide web", *The Guardian*, 21-jun-2013. [En

línea]. Disponible en: https://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. [Consultado: 07-feb-2017].
[49] "FY2013 Foreign Partner Review". [En línea]. Disponible en: https://edwardsnowden.com/2014/06/14/fy2013-foreign-partner-review/. [Consultado: 01-jul-2017].
[50] Appelbaum, Jacob *et al.*, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin - SPIEGEL ONLINE - International", *SPIEGEL ONLINE*, 27-oct-2013. [En línea]. Disponible en: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html. [Consultado: 11-may-2017].
[51] S. Maurizi y G. Greenwald, "Revealed: How the Nsa Targets Italy", *l'Espresso*, 05-dic-2013. [En línea]. Disponible en: http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428. [Consultado: 15-may-2017].
[52] "SCS Operations in Italy". [En línea]. Disponible en: https://edwardsnowden.com/2013/12/07/scs-operations-in-italy/. [Consultado: 17-may-2017].
[53] A. Delgado, "¿Espionaje a los quiteños desde la embajada de Estados Unidos?", *Andrés Delgado*, 26-abr-2014. [En línea]. Disponible en: http://andres.delgado.ec/2014/04/26/espionaje-embajada-estadosunidos-quito-celulares-paneles-dielectricos/. [Consultado: 19-may-2017].
[54] D. Campbell, "The Eavesdroppers", may-1976. [En línea]. Disponible en: http://www.duncancampbell.org/menu/journalism/timeout/Eavesdroppers.pdf.
[55] D. Campbell, "They've got it taped", 12-ago-1988. [En línea]. Disponible en: http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf.
[56] McCarthy Kieren, "This is how we know Echelon exists", 14-nov-2001. [En línea]. Disponible en: https://www.theregister.co.uk/2001/09/14/this_is_how_we_know/. [Consultado: 16-jul-2017].
[57] D. Campbell, "My Life Unmasking British Eavesdroppers", *The Intercept*, 08-mar-2015. [En línea]. Disponible en: https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/. [Consultado: 17-jul-2017].
[58] D. Campbell, "NSA: 'yes, there is an ECHELON system' | DuncanCampbell.org". [En línea]. Disponible en: http://www.duncancampbell.org/content/nsa-yes-there-echelon-system. [Consultado: 17-jul-2017].
[59] Gallagher, Ryan, "The NSA's British Base at the Heart of U.S. Targeted Killing", *The Intercept*, 06-sep-2016. [En línea]. Disponible en: https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/. [Consultado: 14-jul-2017].
[60] "Primary FORNSAT Collection Operations". [En línea]. Disponible en: https://edwardsnowden.com/2014/07/23/primary-fornsat-collection-operations/. [Consultado: 17-jul-2017].
[61] M. Aid, "Inside the NSA's Ultra-Secret China Hacking Group", *Foreign Policy*, 10-jun-2013. [En línea]. Disponible en: https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/. [Consultado: 27-jul-2017].
[62] Appelbaum, Jacob, L. Poitras, Laura, M. Rosenbanch, Stöcker, Christian, Schindler, Jörg, y Stark, Holger, "Inside TAO : Documents Reveal Top NSA Hacking Unit (part 1)", *Spiegel Online*, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html. [Consultado: 01-jul-2017].
[63] B. Gellman y E. Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show", *Washington Post*, 30-ago-2013. [En línea]. Disponible en: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-

show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html. [Consultado: 01-jul-2017].
[64] Appelbaum, Jacob, Poitras, Laura, M. Rosenbanch, Stöcker, Christian, Schindler, Jörg, y H. Stark, Holger, “Inside TAO : Documents Reveal Top NSA Hacking Unit (part 3)”, *Spiegel Online*, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html. [Consultado: 01-jul-2017].
[65] B. Gellman y A. Soltani, “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say”, *Washington Post*, 30-oct-2013. [En línea]. Disponible en: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html. [Consultado: 14-jul-2017].
[66] C. Timberg, B. Gellman, y A. Soltani, “Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic”, *Washington Post*, 26-nov-2013. [En línea]. Disponible en: https://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html. [Consultado: 30-jul-2017].
[67] B. Gellman, Lindenman, Todd, y Ashkan, Soltani, “How the NSA is infiltrating private networks”, *Washington Post*, 30-oct-2013. [En línea]. Disponible en: https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-infiltrating-private-networks/542/. [Consultado: 30-jul-2017].
[68] A. Müller-Maguhn, L. Poitras, M. Rosenbach, M. Sontheimer, y C. Grothoff, “Treasure Map: The NSA Breach of Telekom and Other German Firms”, *Spiegel Online*, 14-sep-2014. [En línea]. Disponible en: http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html. [Consultado: 28-jul-2017].
[69] “Satellite Transport Knowledge”. [En línea]. Disponible en: https://edwardsnowden.com/2014/09/15/satellite-transport-knowledge/. [Consultado: 28-jul-2017].
[70] S. O. Germany Hamburg, “Shopping for Spy Gear: Catalog Advertises NSA Toolbox - SPIEGEL ONLINE - International”, *SPIEGEL ONLINE*, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html. [Consultado: 09-feb-2017].
[71] “ANT Product Data”. [En línea]. Disponible en: https://edwardsnowden.com/2013/12/31/ant-product-data/. [Consultado: 22-sep-2017].
[72] “Stealthy Techniques Can Crack Some of SIGINT’s Hardest Targets | Courage Snowden”. [En línea]. Disponible en: https://edwardsnowden.com/2014/05/14/stealthy-techniques-can-crack-some-of-sigints-hardest-targets/. [Consultado: 01-jul-2017].
[73] “Intercept with PGP encrypted message”. [En línea]. Disponible en: https://edwardsnowden.com/2015/01/06/intercept-with-pgp-encrypted-message/. [Consultado: 22-sep-2017].
[74] “Intercept with OTR encrypted chat”. [En línea]. Disponible en: https://edwardsnowden.com/2015/01/07/intercept-with-otr-encrypted-chat/. [Consultado: 22-sep-2017].
[75] “Tor Stinks”. [En línea]. Disponible en: https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/. [Consultado: 22-sep-2017].
[76] Appelbaum, Jacob *et al.*, “Prying Eyes: Inside the NSA’s War on Internet Security”, *SPIEGEL ONLINE*, 28-dic-2014. [En línea]. Disponible en: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html. [Consultado: 03-ene-2017].

[77] J. Ball, J. Borger, y G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, 06-sep-2013. [En línea]. Disponible en: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. [Consultado: 29-sep-2017].
[78] N. Perlroth, J. Larson, y S. Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web", *The New York Times*, 05-sep-2013. [En línea]. Disponible en: https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. [Consultado: 29-sep-2017].
[79] J. Larson, "Revealed: The NSA's Secret Campaign to Crack, Undermine…", *ProPublica*, 05-sep-2013. [En línea]. Disponible en: https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption. [Consultado: 29-sep-2017].
[80] "Intelligently filtering your data: Brazil and Mexico case studies". [En línea]. Disponible en: https://edwardsnowden.com/2013/12/18/intelligently-filtering-your-data-brazil-and-mexico-case-studies/. [Consultado: 10-may-2017].
[81] "X-KEYSCORE as a SIGDEV tool". [En línea]. Disponible en: https://edwardsnowden.com/2015/07/22/x-keyscore-as-a-sigdev-tool/. [Consultado: 03-mar-2017].
[82] B. M. Tecnología, "La poderosa herramienta de EE.UU. para vigilarlo todo en internet", *BBC Mundo*, 08-ene-2013. [En línea]. Disponible en: http://www.bbc.com/mundo/noticias/2013/08/130801_tecnologia_snowden_nsa_xkeyscore_dp. [Consultado: 22-abr-2017].
[83] G. Greenwald, E. MacAskill, y L. Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, 11-jun-2013.
[84] "XKeyScore". [En línea]. Disponible en: https://edwardsnowden.com/2013/07/31/xkeyscore-training-materials/. [Consultado: 01-ago-2017].
[85] "XKEYSCORE, Cipher Detection, and You!" [En línea]. Disponible en: https://edwardsnowden.com/2015/08/11/xkeyscore-cipher-detection-and-you/. [Consultado: 08-ago-2017].
[86] M. Marquis-Boire, G. Greenwald, y L. Micah, "NSA's Google for the World's Private Communications", *The Intercept*, 01-jul-2015. [En línea]. Disponible en: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/. [Consultado: 02-feb-2017].
[87] "Using XKEYSCORE to Enable TAO". [En línea]. Disponible en: https://edwardsnowden.com/2015/07/21/using-xkeyscore-to-enable-tao/. [Consultado: 23-sep-2017].
[88] "Introduction to XKS Application IDs and Fingerprints". [En línea]. Disponible en: https://edwardsnowden.com/2015/07/14/introduction-to-xks-application-ids-and-fingerprints/. [Consultado: 04-ago-2017].
[89] "The Unofficial XKEYSCORE User Guide". [En línea]. Disponible en: https://edwardsnowden.com/2015/07/15/the-unofficial-xkeyscore-user-guide/. [Consultado: 04-ago-2017].
[90] Kao, Evelyn, "Making search more secure", *Official Google Blog*, 18-oct-2011. [En línea]. Disponible en: https://googleblog.blogspot.com/2011/10/making-search-more-secure.html. [Consultado: 14-feb-2017].
[91] Schillace, Sam, "Default https access for Gmail", *Official Gmail Blog*, 01-dic-2010. [En línea]. Disponible en: https://gmail.googleblog.com/2010/01/default-https-access-for-gmail.html. [Consultado: 14-feb-2017].
[92] Aas, Josh, "Milestone: 100 Million Certificates Issued - Let's Encrypt - Free SSL/TLS Certificates", 28-jun-2017. [En línea]. Disponible en: https://letsencrypt.org/2017/06/28/hundred-million-certs.html. [Consultado: 08-ago-2017].
[93] "Electrospaces.net: Section 215 bulk telephone records and the MAINWAY database", *Electrospaces.net*, 20-ene-2016. [En línea]. Disponible en:

https://electrospaces.blogspot.com.ar/2016/01/section-215-bulk-telephone-records-and.html. [Consultado: 08-ago-2017].
[94] J. Ball, “NSA stores metadata of millions of web users for up to a year, secret files show”, *The Guardian*, 30-sep-2013. [En línea]. Disponible en: http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents. [Consultado: 09-ago-2017].
[95] “User’s Guide for PRISM Skype Collection”. [En línea]. Disponible en: https://edwardsnowden.com/2015/01/05/users-guide-for-prism-skype-collection/. [Consultado: 09-ago-2017].
[96] G. Greenwald, “XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’”, *The Guardian*, 31-jul-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. [Consultado: 02-feb-2017].
[97] “Serving our customers”. [En línea]. Disponible en: https://edwardsnowden.com/2014/06/14/serving-our-customers/. [Consultado: 22-sep-2017].
[98] L. Poitras, M. Rosenbanch, y H. Stark, “GCHQ and NSA Targeted Private German Companies and Merkel”, *SPIEGEL ONLINE*, 29-mar-2014. [En línea]. Disponible en: http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html. [Consultado: 10-may-2017].
[99] “Content Extraction Analytics”, *Content Extraction Analytics*, 21-may-2009. [En línea]. Disponible en: https://edwardsnowden.com/2014/06/26/content-extraction-analytics/.
[100] “Veja os documentos ultrassecretos que comprovam espionagem a Dilma”, *Fantástico*, 02-sep-2013. [En línea]. Disponible en: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html. [Consultado: 05-may-2017].
[101] S. O. Germany Hamburg, “Fresh Leak on US Spying: NSA Accessed Mexican President’s Email - SPIEGEL ONLINE - International”, *SPIEGEL ONLINE*, 20-oct-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html. [Consultado: 09-feb-2017].
[102] “Computer-Network Exploitation Successes South of the Border”, 15-nov-2010. [En línea]. Disponible en: https://edwardsnowden.com/2015/01/30/computer-network-exploitation-successes-south-of-the-border/. [Consultado: 26-may-2017].
[103] Fishman, Andrew y G. Greenwald, “Britain Used Spy Team to Shape Latin American Public Opinion on Falklands”, 02-abr-2015. [En línea]. Disponible en: https://theintercept.com/2015/04/02/gchq-argentina-falklands/. [Consultado: 01-jul-2017].
[104] “#EspiadosPorLosIngleses: los nuevos documentos de Snowden revelan un plan de espionaje de Gran Bretaña en Argentina por Malvinas - TN.com.ar”, *Todo Noticias*, 02-abr-2015. [En línea]. Disponible en: http://tn.com.ar/politica/espiadosporlosingleses-los-nuevos-documentos-de-snowden-revelan-un-plan-de-espionaje-de-gran-bretana_580250. [Consultado: 17-sep-2017].
[105] “JTRIG Operational Highlights, August 2009”. [En línea]. Disponible en: https://edwardsnowden.com/2015/04/08/jtrig-operational-highlights-august-2009/. [Consultado: 17-sep-2017].
[106] M. Vann, “Exclusive: Snowden Docs Show British Spies Used Sex and ‘Dirty Tricks’”, *NBC News*, 07-feb-2014. [En línea]. Disponible en: https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091. [Consultado: 17-sep-2017].
[107] E. Magnani, “WIndows 10 y plan Sarmiento – Esteban Magnani”, 20-sep-2017. [En línea]. Disponible en: http://www.estebanmagnani.com.ar/2017/09/20/windows-10-y-plan-sarmiento/. [Consultado: 24-sep-2017].

[108] “SIGDEV: Is It Time for a ‘Target Reboot’?”, 23-mar-2011. [En línea]. Disponible en: https://edwardsnowden.com/2015/11/18/sigdev-is-it-time-for-a-target-reboot/.

[109] Greenwald, Glenn y Fishman, Andrew, “Overwhelmed NSA Surprised to Discover Its Own Surveillance ‘Goldmine’ on Venezuela’s Oil Executives”, *The Intercept*, 18-nov-2015. [En línea]. Disponible en: https://theintercept.com/2015/11/18/overwhelmed-nsa-surprised-to-discover-its-own-surveillance-goldmine-on-venezuelas-oil-executives/. [Consultado: 26-may-2017].

[110] “American and Canadian Spies target Brazilian Energy and Mining Ministry”, *Fantástico*, 06-oct-2013. [En línea]. Disponible en: http://g1.globo.com/fantastico/noticia/2013/10/american-and-canadian-spies-target-brazilian-energy-and-mining-ministry.html. [Consultado: 26-may-2017].

[111] “I Hunt Sys Admins”. [En línea]. Disponible en: https://edwardsnowden.com/2014/03/21/i-hunt-sys-admins/. [Consultado: 13-sep-2017].

[112] Gallagher, Ryan, “Inside the NSA’s Secret Efforts to Hunt and Hack System Administrators”, *The Intercept*, 20-mar-2014. [En línea]. Disponible en: https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/. [Consultado: 28-jul-2017].

General

- American Civil Liberties Union, “NSA Documents”, American Civil Liberties Union. [En línea]. Disponible en: https://www.aclu.org/nsa-documents-search. [Consultado: 26-sep-2017].
- Courage Foundation, “Courage Snowden”. [En línea]. Disponible en: https://www.edwardsnowden.com/. [Consultado: 26-sep-2017].
- Der Spiegel, “NSA Spying Scandal - SPIEGEL ONLINE”. [En línea]. Disponible en: http://www.spiegel.de/international/topic/nsa_spying_scandal/. [Consultado: 26-sep-2017].
- Electronic Frontier Foundation, “NSA Primary Sources”, Electronic Frontier Foundation, 19-nov-2013. [En línea]. Disponible en: https://www.eff.org/nsa-spying/nsadocs. [Consultado: 26-sep-2017].
- E. Magnani, Tensión en la red: libertad y control en la era digital. 2014.
- B. Schneier, “Schneier on Security: Blog Entries Tagged NSA”. [En línea]. Disponible en: https://www.schneier.com/cgi-bin/mt/mt-search.cgi?search=NSA&__mode=tag&IncludeBlogs=2&limit=10&page=1. [Consultado: 26-sep-2017].
- The Guardian, “The NSA files”, the Guardian. [En línea]. Disponible en: http://www.theguardian.com/us-news/the-nsa-files. [Consultado: 26-sep-2017].
- The Intercept, “Documents - The Intercept”. [En línea]. Disponible en: https://theintercept.com/documents/. [Consultado: 29-sep-2017].

Índice de Imágenes

Índice de Imágenes